NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 104627A
9 November 2019

MUCKROCK
DEPT MR 56530
411A HIGHLAND AVE.
SUMMERVILLE, MA 02144-2516

Dear Emma Best:

This responds to your Freedom of Information Act (FOIA) request of 20 June 2018, for "Copies of initial emails (not including replies) sent to tech_transfer@nsa.gov from 2010 to the present." Your request was received on 21 June 2018, and has been assigned Case Number 104627. There are no assessable fees for this request; therefore, we did not address your fee category or your request for a fee waiver.

Your request has been processed under the FOIA and some of the documents you requested are enclosed. Certain information, however, has been deleted from the enclosures and some documents containing commercial and financial information that is privileged or otherwise confidential have been withheld in their entirety pursuant to the fourth exemption of the FOIA.

During the course of our search it was discovered that the Technology Transfer Program (TTP) established their mail feature in 2012. Thus only records from 2012 through 2018 are enclosed. However, certain information has been deleted from the enclosures.

Information which would reveal NSA/CSS functions and activities and names of NSA/CSS employees have been deleted from the enclosures. These deletions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable in this case is Section 6, Public Law 86-36 (50 U.S. Code 3605).

In addition, commercial and financial information that is privileged or otherwise confidential has been deleted from the enclosures, pursuant to the fourth exemption of the FOIA.

In addition, some of the information has been deleted from the enclosures pursuant to the fifth exemption of the FOIA. This exemption applies to inter-agency or intra-agency memoranda or letters which would not be available by law to a party in litigation with the agency, protecting information that is normally privileged in the civil discovery context, such as information that is part of a pre-decisional deliberative process.

Finally, personal information regarding an individual has been deleted from the enclosures in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

Since some documents were withheld in their entirety and information was withheld from the enclosures, you may construe this as a partial denial of your request. You are hereby advised of this Agency's appeal procedures.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

  NSA FOIA/PA Appeal Authority (P132)
  National Security Agency
  9800 Savage Road STE 6932
  Fort George G. Meade, MD 20755-6932

  The facsimile number is 443-479-3612.
  The appropriate email address to submit an appeal is FOIARSC@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the

National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877-684-6448
(Fax) 202-741-5769

Sincerely,

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

Doc ID: 6687022

(b)(3)-P.L. 86-36

From: [redacted]
To:
Subject: (U) 2-Day Notification: [redacted] Unclass Exchange 2010 Mailbox Migration Will Begin at 1600 hours (4:00 p.m.) on Sunday (August 5, 2012)
Date: Thursday, August 02, 2012 8:52:05 AM

(U//~~FOUO~~) This is a reminder that [redacted] will be migrating your unclassified mailbox to an Exchange 2010 server. There will be no changes made to your Outlook mailbox (or to your desktop). The migration will take approximately 4-5 hours. After that time, you may reopen your Outlook or log back in at the start of your next work day.

(U) What do I need to do for the migration?

(U//~~FOUO~~) IF you cannot be migrated on the above date due to mission reasons, please email the [redacted] in order to reschedule. If you have any issues after the migration or need more information, please email the [redacted] at [redacted] You may also contact the Information Technology Support Center (ITSC) by calling [redacted]

Thank you.

[redacted]

(b)(3)-P.L. 86-36

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Action, Response Requested: Patent Searching via Visualization
Date: Monday, November 26, 2012 12:27:37 PM
Importance: High

To Whom It May Concern:

My name is [redacted] and I am a Commercialization Manager in the Technology Transfer department at the Department of Energy's Pacific Northwest National Laboratory in Richland, Washington.

I am writing to request a quick call with the Technology Transfer representative who is responsible for the marketing and communications of available technologies in your department. The Lab recently completed a project which categorizes and visualizes all of the DOE's active patent and patent applications. The goal being, make available technologies more accessible to technology seekers. The Visual Patent Search tool is available for viewing at: https://techportal.eere.energy.[illegible]gov/visual_patent_search/

During the call I would like to know whether the framework would help you organize your patents for technology seekers looking to license innovations.

Please suggest 2-3 meeting times over the next two weeks that may work for your schedule. Also, feel free to give me a call at [redacted] to schedule.

Thanks,

(b) (6)

[redacted]

[redacted]
Commercialization Manager
Technology Commercialization
Pacific Northwest National Laboratory
902 Battelle Boulevard
P.O. Box 999, MSIN K1-71
Richland, WA 99352 USA
[redacted]
[redacted]
www.pnnl.gov

PNNL's Available Technologies website provides searchable access to our ever-growing collection of licensable technologies! Visit the site to browse currently available technologies or to learn more about what we might be able to develop together as research partners.

[illegible] for [illegible]

(b) (6)

From: [redacted]
Sent: Thursday, October 18, 2012 12:12 PM
To: Tech_Transfer
Subject: Encrypted DNA tags (UNCLASSIFIED)
Attachments: Encrypted DNA Tags Overview V1.pptx

Importance: High

Classification: UNCLASSIFIED
Caveats: ~~FOUO~~

Dear NSA Tech Transfer folks,

Our bio folks have come up with a DNA based marking technology which can be used for anti-counterfeiting, supply chain tracking, other places where you want to verify that something on one end is the same as at the other end, etc. Perhaps could even be used to mark computer chips to ensure they are not counterfeit. ...

They are looking to see if anyone in the IC would have any interest in using/co-developing its application.

Please let me know if you would like some more information on it.

(b) (6)

[redacted]
Senior Intelligence Officer
Edgewood Chemical Biological Center
[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, October 10, 2012 12:22 PM
To: [redacted]
Cc: [redacted]
Subject: Encrypted DNA tags (UNCLASSIFIED)
Importance: High

Classification: UNCLASSIFIED
Caveats: ~~FOUO~~

Gentlemen:

[redacted]

This project to create unbreakable DNA tags to ensure item "authenticity" is a high priority for us to get funded. We feel it has tremendous potential. Can you help us? You may forward this as you deem appropriate.

DESCRIPTION:
Edgewood scientists have exploited DNA's intrinsic ability to "store" information to construct small unbreakable DNA tags that can be affixed to materials to ensure chain of custody and authenticity in the field. These nano-scale devices can transduce the presence or absence of a very specific DNA sequence (information) into a readily-observable property (light) without the need for hardware beyond a blue penlight. We have demonstrated the immobilization of these strand-displacement devices on a nitrocellulose membrane and further established the selective activation of these devices through the addition of the correct "message" DNA sequences to a drop of buffer applied to the surface. This DNA tag represents a significant improvement over currently employed DNA tags because it does not require time consuming interpretation in a sequencing laboratory at high expense. Instead a DNA tag can be read within minutes in the field through the use of a disposable test kit the size of a stick of gum.

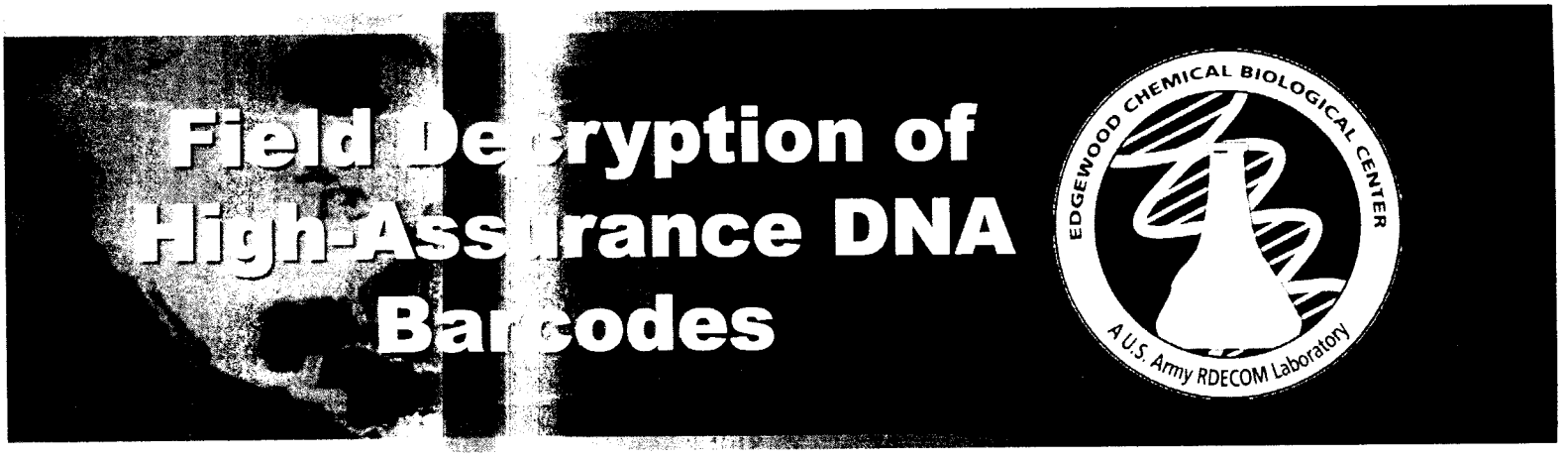
We propose to deliver a tamper resistant DNA tagging system that can be read with small hand held assay costing $5. The project will demonstrate the secure nature and perform a pilot study on a collection of DNA tags and effectively demonstrate utility and cost effectiveness in comparison to currently employed strategies.

Classification: UNCLASSIFIED
Caveats: ~~FOUO~~

Classification: UNCLASSIFIED
Caveats: ~~FOUO~~

Doc ID: 6687057

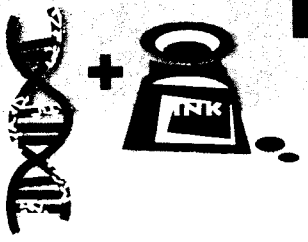
US ARMY RDECOM



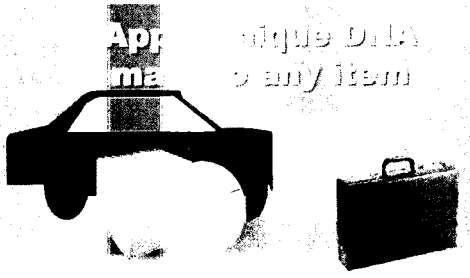
TECHNOLOGY DRIVEN.

ECBC's Encrypted DNA (EDNA) Barcode Technology

Secure design and production of DNA and test strips

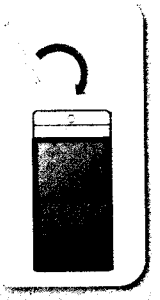


Apply unique DNA to any item



Locate and swab marked unique DNA

Place swab in pouch with test strip



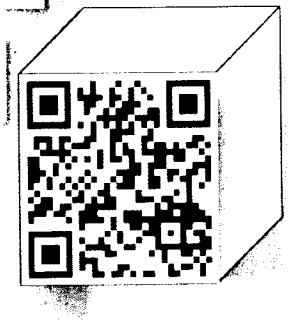
Pattern develops in 5-10 minutes

Information in the DNA decrypted by EDNA test strip

Item verified in the field

Additional Levels of Security Available if Required

SECURE
message, item or
document
verified



WARFIGHTER FOCUSED.

U.S. ARMY

ECBC's DNA Encryption Program:

ECBC's new DNA Encr tion Program will be able to provide the ultimate encrypted-DN solutions designed to provide the highest level of security. From mark g individual items to authenticating secure government documen

The Advantages of DNA Encryption Markers:

- Highly resistant to reverse engineering or duplication
- Verified with cheap, disposable hand held test kit
- Unique tagging is possible to achieve 'one-time pad' security
- ***Covert*** or ***overt***, DNA sequences are acceptable forensic evidence
- Custom DNA marks and strips can be created for specific needs
- Compatible with a wide range of handling and manufacturing processes

WARFIGHTER FOCUSED.

Commercial vs. ECBC EDNA Barcode Technology

Requirements	Commercial DNA Barcodes	EDNA Barcodes
Security	High (single level)	High (**multiple** levels)
Time	2 week, off-site verification	**10 minutes**, on-site verification
Cost	Expensive for routine use – PCR, custody chain to lab	**Inexpensive** - disposable assay strip can be made for pennies
Resources	**Requires laboratory** for definitive verification	**On-site results** using test strip, assays available for fielded PCR
Production	Commercial/Foreign	Commercial or **DoD secure**

Sec rity Tailored to Need

U.S. ARMY ID: 6687057

Lower

Price, operational load

Higher

Operational Considerations

Difficulty to Spoof

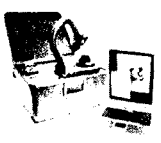
Lower

Need for security

Higher

1. tar UPC labels
- h-sp ction

2. tra isplacement Technology
- nd-h wer free, yes/no answer
- say
- ique



3. Fiel PCR machines
- d ac l message and noise DNA
- R d of low abundance message
- der in field requires equipment

4. Ger ic Sequencing
- DNA a al storage, info in sequences
- S curi strong as your digital encryption
- R quir -site processsing (~2 weeks)

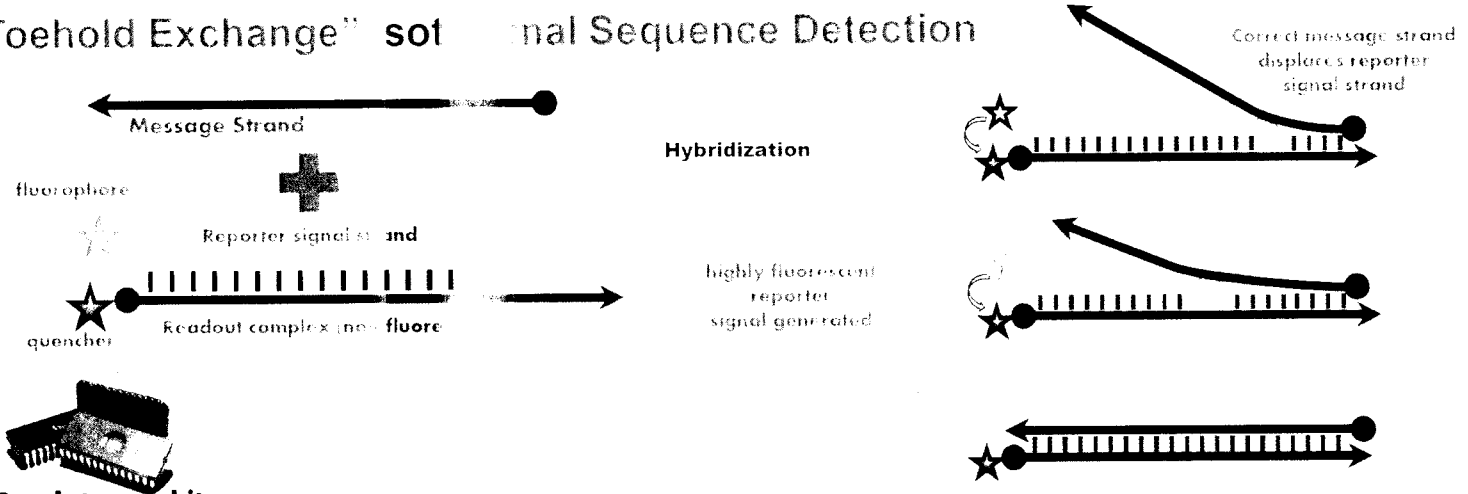
Sequence, synthesize
- Could be copied at great expense (as above) but system is as spoof-resistant as the encryption used.

WARFIGHTER FOCUSED.

U.S. ARMY
IDTECOM

How Does Strand Displacement Work

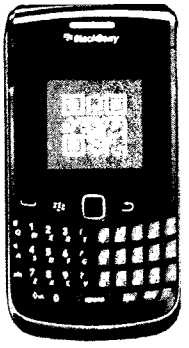
"Toehold Exchange" sot nal Sequence Detection

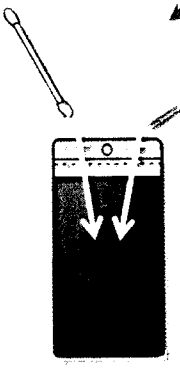


Swab tagged item and place in hybridization Pouch with test ticket

Test ticket contains array of multiple readout complexes

Smartphone Image ticket





Co-incubation with correct messages develops the correct pattern

"Peel and stick" disposable filters enable flash and camera to detect fluorescence.

Verification of Pattern in software.

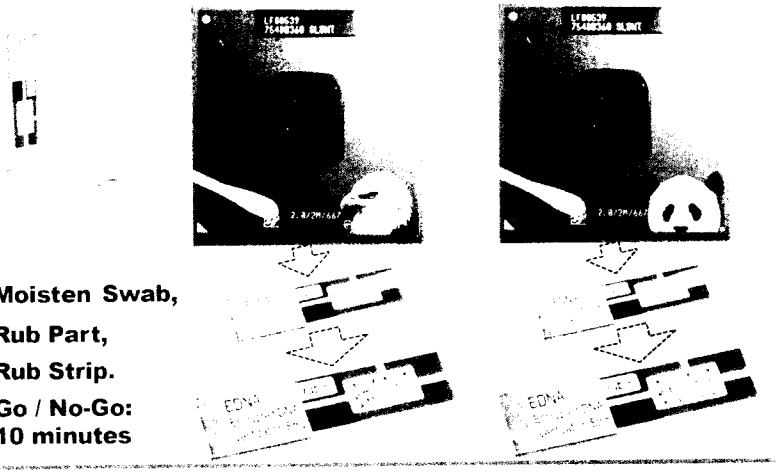
Verification of item in ~20 minutes

WARFIGHTER FOCUSED.

Field Decryption of High-Assurance DNA messages

Objective: Secure and increase end-user confidence in the supply chain by developing high-assurance DNA anticounterfeiting marks and a disposable, cheap means for their verification.

Description of the effort: An algorithm will be developed to generate a pool of short DNA sequences. These sequences will be used to drive the independent development of pixels on a detection strip. Complex mixtures of these sequences will be used to mark an item. Pattern formation on the strip will require only application of the DNA from the item.

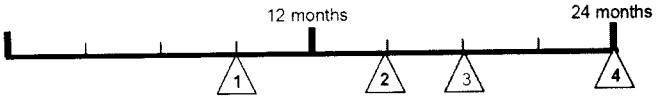


Benefits: An inexpensive means of verification enables more frequent testing and higher confidence in the supply chain. Technology is adaptable to existing "DNA ink" nanoencapsulation technologies and printing methods. Pattern on test strip could be both human-readable and machine-readable. Additional layers of security easily applied down to encrypting information in the barcode on a per-item basis.

Challenges: Cross-talk between sequences/pixels is possible. Deliberate contamination could render DNA marks unreadable. Copying of DNA marks while expensive and exceptionally difficult could be possible.

Maturity: Working 2-pixel proof of concept.

Major Tasks:
Task 1: Deliver validated design rules
Task 2: Synthesize flourophore-modified oligos
Task 3: Select material for test ticket, incorporate DNA tag into ink
Task 4: Technology Demonstration



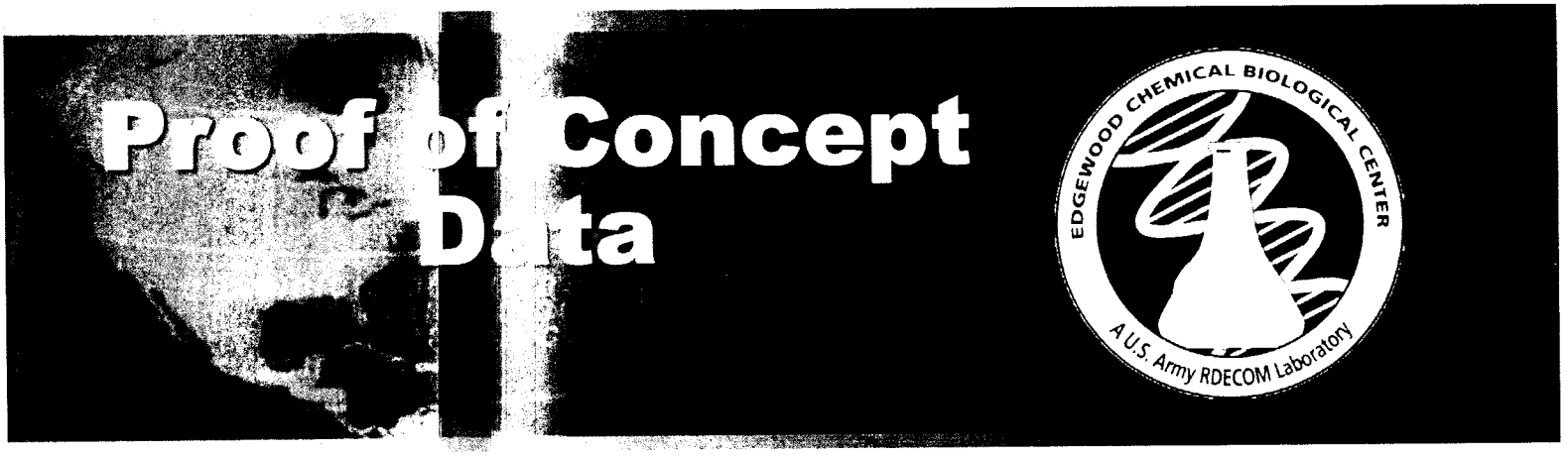
Proposed Funding: **Year 1**: $552K **Year 2**: $661K

PI contact info:
Dr. [redacted]
US Army Edgewood Chemical Biological Center
[redacted]

WARFIGHTER FOCUSED.

Doc ID: 6687057

US ARMY RDECOM



TECHNOLOGY DRIVEN.

Making the Test Ticket

Spotfluorescent oligo on ticket. 0.3µL of 100pmol/µL solution in diH20. Let dry.

1 2

Wash in shallow pan of diH20 1 hour to remove unbound oligo.

1 2

Overlay fluorescent spots with 0.5µL of 100pmol/µL quencher (with 10mM MgSO4). Spot appears pink, no longer fluorescent.

1 2

Immediately wash overnight in shallow pan of 10mM TRIS, 4mM MgSO4, pH 7.7. Spot is less pink, still nonfluorescent. Air dry, then ready to test.

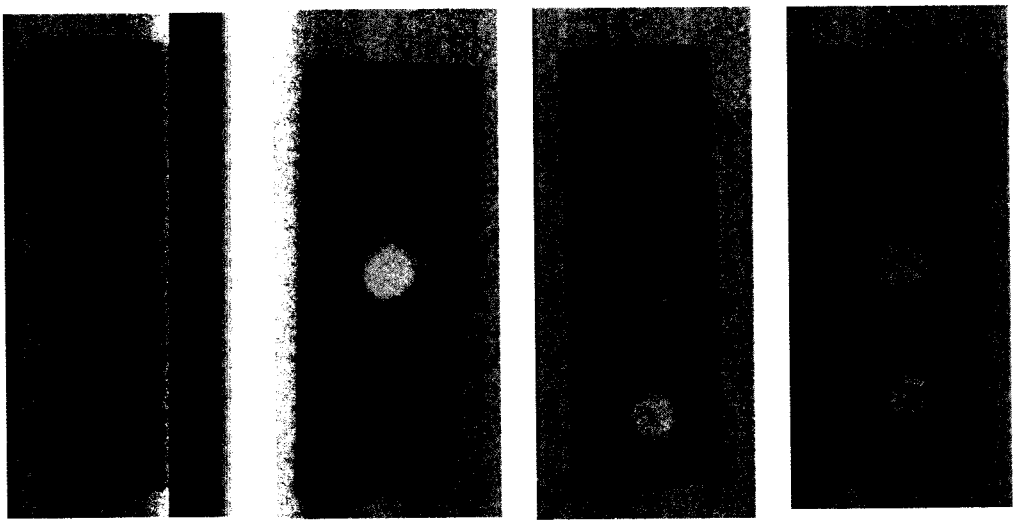
1 2

Quencher 1 added to Fluor 1, Quencher 2 added to Fluor 2.

Tested Q1 on F2 / Q2 on F1 – doesn't quench effectively and washes away overnight leaving behind a fluorescent spot (does not hybridize to the fluorescent strand!)

2-pixel Test Ticket

Test ticket resolving 2 different oligos using the strand displacement method saw no crosstalk with signal appearing *in under 5 minutes*



Buffer control (TRIS/MgSO4) | Oligo A | Oligo B | Oligo A & B

Oligos at 5 pmol/µL

Blue backlight 580nm filter

t=5 min

WARFIGHTER FOCUSED.

Doc ID: 6687058

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: NSA Technology Detects Intermediary Computers on Network
Date: Tuesday, September 11, 2012 10:11:05 AM

To whom it may concern,

I am looking for any and all information you can provide me on the technology that detects intermediary computers on a network. If it helps, I am a subcontractor for the Department of Energy.

Thanks,

(b) (6)

[redacted], CISSP
IT Manager, Cyber Security
Information Security Site Manager (ISSM)
National Nuclear Security Administration's Kansas City Plant
Operated by Honeywell Federal Manufacturing & Technologies, LLC
Office: [redacted]
Pager: [redacted]
Blackberry: [redacted]
www.kcp.com

[redacted]

Doc ID: 6687059

(b)(3)-P.L. 86-36

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: USSTRATCOM interest in Tech Transfer Program
Date: Tuesday, October 23, 2012 4:50:47 PM

Hello TTP representative,

Here at US Strategic Command we have recently begun contract with an University Affiliated Research Center (UARC) with Nebraska University. Within this UARC we have a set of USSTRATCOM Core Competencies that the university will research; much like the NSA key areas of expertise (acoustics, communications, advanced mathematics, computer technology, etc) I would like to expand on ways that the USSTRATCOM UARC would conduct collaborative research with NSA. I heard about this in "The Next Wave" Vol.19, No.3, 2012 magazine. Of particular interest, would be the Cooperative Research and Development Agreements (CRADAs). Who would be the best person to talk to concerning establishing joint research and development efforts?

V/r,

(b)(3)-P.L. 86-36

[redacted]
CWMD Program Analyst
USSTRATCOM. J85 CWMD
Capabilities Integration
[redacted]

"Great discoveries and improvements invariably
involve the cooperation of many minds." --Alexander Graham Bell

[redacted]

Doc ID: 6687060

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Request - Process to Obtain NSA TTSA
Date: Tuesday, May 07, 2013 5:05:43 PM

[redacted] and/or FTP Representative: (b) (3)-P.L. 86-36

In the past, my squadron had an agreement with NSA to share applications.

We would like to obtain authorization to use the following NSA applications: SIMP, Niagara Files, RYA, GI M ALX, REX, and Renoir.

The only application that exists on your website is Renoir.

What is the current process to request these NSA applications? Do you have a standard Technology Transfer Sharing Agreement form? Or do we just reuse a past agreement spelling out these applications?

Thank you for your time.

(b) (6)

[redacted]
92 IOS/OSF, Interoperability
[redacted]

[redacted]

Doc ID: 6687061

(b) (6)

From: [redacted] (b) (3)-P.L. 86-36
To: [redacted] Tech Transfer
Cc: [redacted]

Subject: Request - Review of Draft 688 IOW TTSA
Date: Monday, May 13, 2013 3:51:13 PM
Attachments: Cyber Pilot TTSA.docx

(b) (6)

[redacted] (b) (3)-P.L. 86-36

Attached is a draft Technology Transfer Sharing Agreement that we would like to initiate.

At your convenience would you review it, and let us know if it acceptable before we send it up for coordination and signature.

(b) (6)

[redacted]

[redacted]

Doc ID: 6687061

(b)(3)-P.L. 86-36
(b)(5)

Page Denied

Doc ID: 6687061

(b)(3)-P.L. 86-36
(b)(5)

Page Denied

Doc ID: 6687062

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: UMD/NSA Jt. Invention Disclosure (UMD PS-2013-085)
Date: Friday, September 06, 2013 2:04:25 PM

Good Afternoon,

Our office has received an invention disclosure which lists an NSA employee as a co-inventor. Below is the pertinent information:

UMD Reference No.: PS-2013-085
Title of Invention: "Plasma-Assisted Smoothing of Photoresist Sidewalls" (b) (3)-P.L. 86-36
Inventors: [redacted] (b) (6)
Sponsor: NSA
NSA Award No.: H98230-12C0256

Could you please let me know who in your office my point of contact would be? Thank you very much for your assistance.

(b) (6)

[redacted]
Coordinator

Please note our new address
Office of Technology Commercialization
University of Maryland
2130 Mitchell Building
College Park, MD 20742

[redacted]

www.otc.umd.edu

[redacted]

Doc ID: 6687063

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: "4d"
Subject: Bayh-Dole reporting for NSA
Date: Thursday, August 21, 2014 6:28:19 PM
Attachments: compliance requirements 14-256.bmp

Hi,

I'm hoping someone can give me some guidance for reporting inventions supported by the NSA. I work at Stanford University in the technology transfer office and am responsible for government reporting per Bayh-Dole. A new technology was recently disclosed to our office and the disclosure indicates support from the NSA. I have attached the section of the contract that discusses the reporting of inventions. The section indicates that the contractor should submit a DD882 to the Director, NSA/CSS with a copy to the Maryland Procurement Office. However, this falls under Section H.2 which deals with Contract Administration and Closeout Guidance. Is there any reporting that needs to be done now or should the DD882 be submitted only when the grant ends? Also, can you please send me the contact information for the individual who should receive Bayh-Dole compliance documents.

Best regards,

(b) (6)

[redacted]
Compliance Manager

[redacted]

(e) Report of Inventions and Subcontracts (Form DD882). Pursuant to the Patent Rights Clause of this contract, the contractor shall submit the DD Form 882 to the Director, NSA/CSS, ATTN: [redacted] R3, 9800 Savage Road, Ft. George G. Meade, Maryland 20755-6000, with a courtesy copy to the MPO (ATTN: BA331 [redacted], Maryland Procurement Office, 9800 Savage Road, Fort George G. Meade, MD 20755-6000).

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Bluescope
Date: Monday, December 15, 2014 12:38:45 PM

What do I need to get a TTA for Bluescope?
We currently have one thought another team member that has left and need to get one in place for myself.

(b) (6)

v/r,
[redacted]
Computer Network Defense (CND)
[redacted]
Patuxent River, MD 20670
[redacted]

[redacted]

Doc ID: 6687065

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: CRADA / PLA agreement inquiry
Date: Friday, June 20, 2014 11:10:56 AM

Hi [redacted] (b) (3)-P.L. 86-36

Is it possible to confirm whether or not someone has worked with the government under a CRADA agreement if they claim to have done so?

The individual's name is [redacted] Here is what [redacted] released as public information:

[redacted] has 16 years experience developing anti-fraud technology related to network transactions and has previously worked with the US National Security Agency under a Co-Operative Research and Development Agreement and Patent License Agreement to develop and commercialize network security related technology"

I'm in the public sector as an investor and I'm looking to inquire if the above claim can be definitely confirmed via website, email or phone call?

Thanks,

[redacted] (b) (6)

Sent from my iPad

[redacted]

Doc ID: 6687066

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: From the Office of Technology Transfer, George Mason University, Website Detection Over a Secure Network, GMU 10-023
Date: Wednesday, September 17, 2014 10:45:01 AM
Attachments: GMU-10-023U 2014-05-13 Issued Patent.pdf

Dear Sir or Madam,

I am contacting you from the Office of Technology Transfer at George Mason University (located in Fairfax, VA). While I know that your office typically handles out licensing of NSA developed technologies I am contacting you because we have a technology that I believe would be of interest to the NSA. Would someone in your office be able to direct me to an appropriate person in the NSA that might be able to evaluate possible interest in our technology? The description of the technology follows and I have attached a copy of the issued patent.

Our technology detects the size, order, and timing descriptions of website packet data to generate a unique "fingerprint" of each site visited over a secure network. The fingerprints are used to search and identify websites inside the encrypted traffic generated by users over time, allowing companies to identify web traffic. What would otherwise be impossible to detect on a secure network becomes available with this technology by "matching" the fingerprints before and after the network to identify communication. Variations on this technology exist, but none are able to generate fingerprints with background noise and dialogue from the server.

I appreciate any help you can give. Please let me know if you would like any additional information or have any questions.

With kind regards,

[redacted]

(b) (6)

[redacted] Market Analyst
Office of Technology Transfer, George Mason University
Phone: [redacted]

[redacted]

Doc ID: 6687066

US008726005B2

(12) **United States Patent**
Stavrou et al.

(10) **Patent No.: US 8,726,005 B2**
(45) **Date of Patent: May 13, 2014**

(54) **WEBSITE MATCHING BASED ON NETWORK TRAFFIC**

(75) Inventors: **Angelos Stavrou**, Springfield, VA (US); **Mohammed A. Alhussein**, McLean, VA (US); **Brian Sanders**, Manassas, VA (US)

(73) Assignee: **George Mason Intellectual Properties, Inc.**, Fairfax, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 146 days.

(21) Appl. No.: **12/965,413**

(22) Filed: **Dec. 10, 2010**

(65) **Prior Publication Data**

US 2011/0314269 A1 Dec. 22, 2011

Related U.S. Application Data

(60) Provisional application No. 61/285,420, filed on Dec. 10, 2009.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
USPC **713/150**; 726/32

(58) **Field of Classification Search**
USPC 713/150; 726/30; 370/390
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,317,693	B1 *	1/2008	Roesch et al.	370/252
7,983,241	B2 *	7/2011	Furuskar et al.	370/352
2003/0074388	A1 *	4/2003	Pham et al.	709/106
2003/0075167	A1	4/2003	Dominguez	
2004/0104807	A1 *	6/2004	Ko	340/5.83
2005/0286145	A1	12/2005	Silhengst	
2006/0233152	A1 *	10/2006	Suda	370/347
2007/0134316	A1	6/2007	Li et al.	
2007/0147041	A1	6/2007	Shiratsuchi	
2008/0092879	A1	4/2008	Dominguez	
2009/0003282	A1 *	1/2009	Meylan et al.	370/331
2009/0077673	A1 *	3/2009	Schmelzer	726/30
2009/0316840	A1 *	12/2009	Park et al.	375/341
2010/0023499	A1 *	1/2010	Johnson et al.	707/5
2010/0030912	A1 *	2/2010	Finkenzeller et al.	709/233
2010/0232431	A1 *	9/2010	Sebastian	370/390
2012/0033558	A1 *	2/2012	Ford et al.	370/241

FOREIGN PATENT DOCUMENTS

DE	202006014814	1/2007
EP	1251366	10/2002
WO	WO 99/14528	3/1999
WO	WO 2009/056000	5/2009

OTHER PUBLICATIONS

Wang Zhulong; Automatic Special type Website Detection Based on Webpage Type Classification; Year:2004; ACM; pp. 1-12.*
Extentended European Search Report issued in EP 11182373.8 on Jan. 30, 2013.

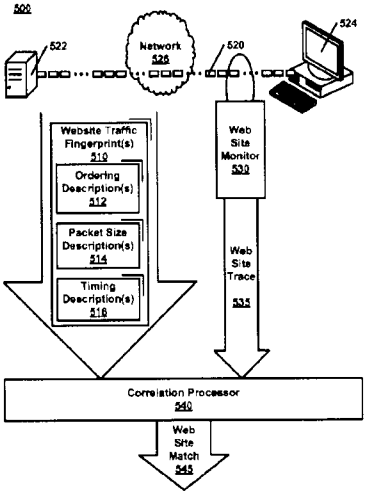
(Continued)

Primary Examiner – Monjour Rahim
(74) *Attorney, Agent, or Firm* DLA Piper LLP (US)

(57) **ABSTRACT**

A website fingerprint is generated that characterizes network traffic associated with a website as a website traffic fingerprint that includes size description(s), order description(s), and timing description(s) of packet traffic for the website. A website monitor generates website trace(s) of packet statistics. A correlation processor correlates a sequence of packet statistics from the website trace(s) with the size description, the order description, and timing description found in the website traffic fingerprint(s).

23 Claims, 7 Drawing Sheets



(56) **References Cited**

OTHER PUBLICATIONS

English Language Abstract of DE 20 2006 014814 published Jan. 4, 2007.

Marc Liberatore, Brian Neil Levine. *Inferring the source of encrypted HTTP connections*. Proceedings of the 13th ACM conference on Computer and communication security. Oct. 30-Nov. 3, 2006, Alexandria, Virginia, USA.

Heyning Cheng, Ron Avnur. *Traffic Analysis of SSL Encrypted Web Browsing*. 1998.

Nguyen T. and Armitage G. *A Survey of Techniques for Internet Traffic Classification Using Machine Learning*. IEEE Communications Survey Tutorials, vol. 10, No. 4. Fourth Quarter. 2008.

Charles Wright, Lucas Ballard, Fabian Monrose, and Gerald Masson. *Language Identification of Encrypted VoIP Traffic*. 16th USENIX Security Symposium, Nov. 2007, Baltimore, Maryland, USA.

Charles Wright, Lucas Ballard, Scott Coulls, Fabian Monrose, and Gerald Masson. *Spot me if you can: recovering spoken phrases in encrypted VoIP conversations*. IEEE Symposium on Security and Privacy, May 2008.

George Dean Bissia, Marc Liberatore, David Jensen, and Brian Neil Levine. *Privacy Vulnerabilities in Encrypted HTTP Streams*, Computer Science Department Faculty Publication Series. Paper 98. 2005.

V.D. Izadinia, D. G. Kourie, and J. H. P. Eloff. *Uncovering identities: A study into vpn tunnel fingerprinting*, Computers and Security, vol. 25, No. 2, pp. 97-105, 2006.

* cited by examiner

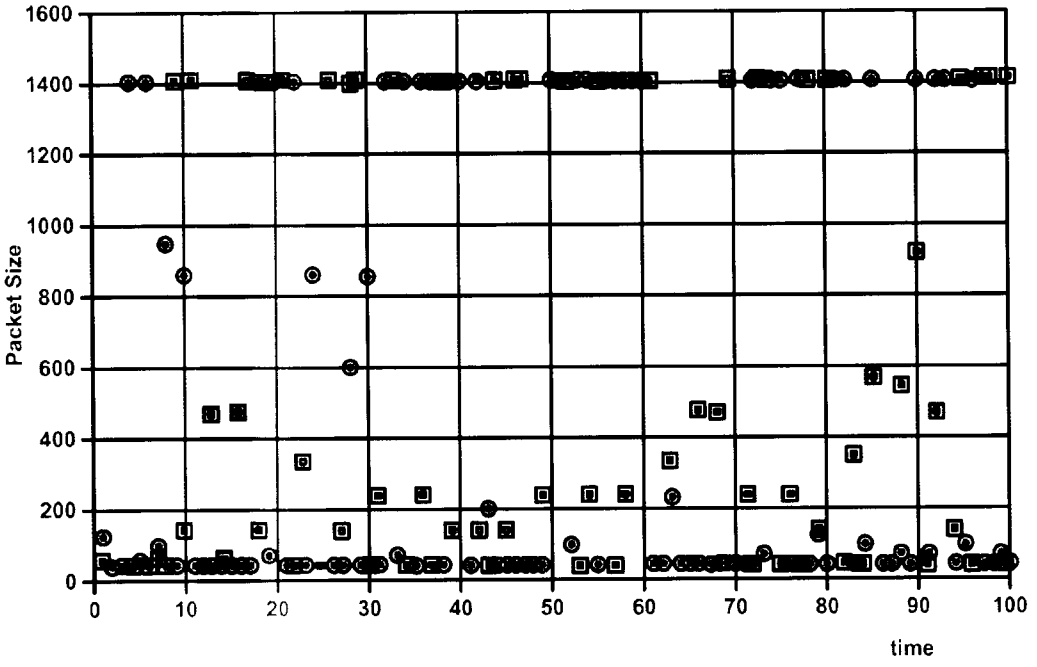

1600
1400
1200
1000
800
600
400
200
0
Packet Size
0
10
20
30
40
50
60
70
80
90
100
time

FIG. 1

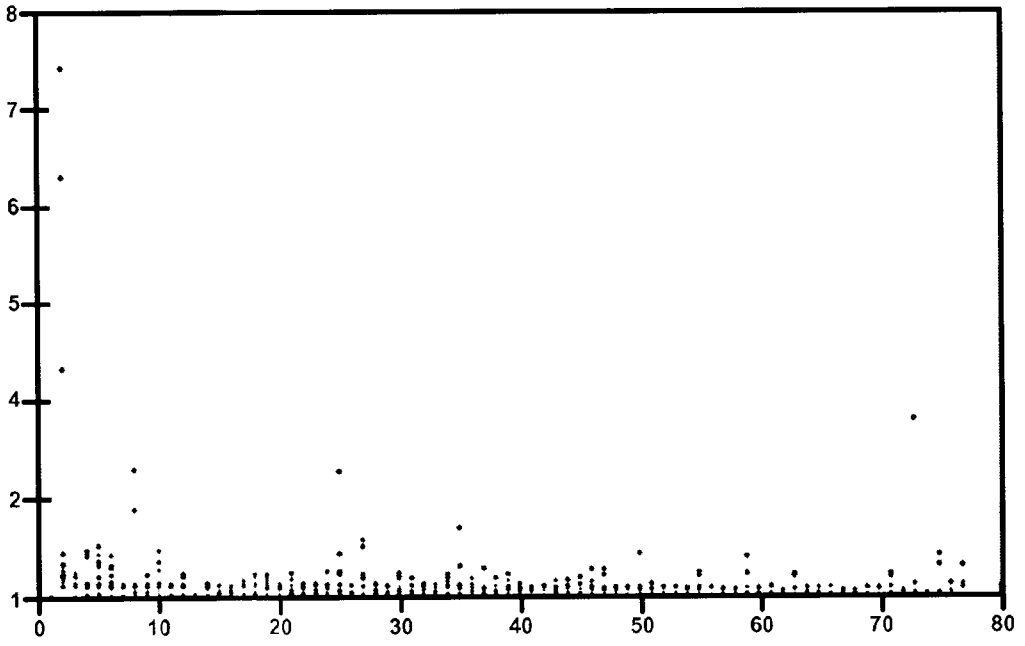


FIG. 2A

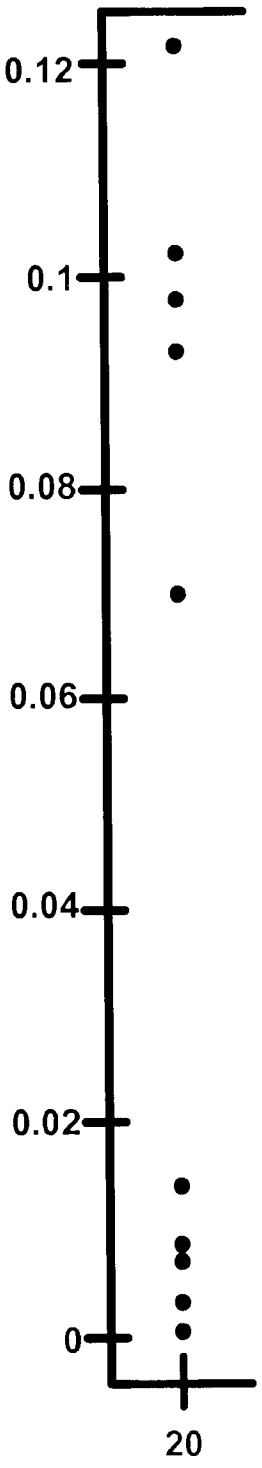


FIG. 2B

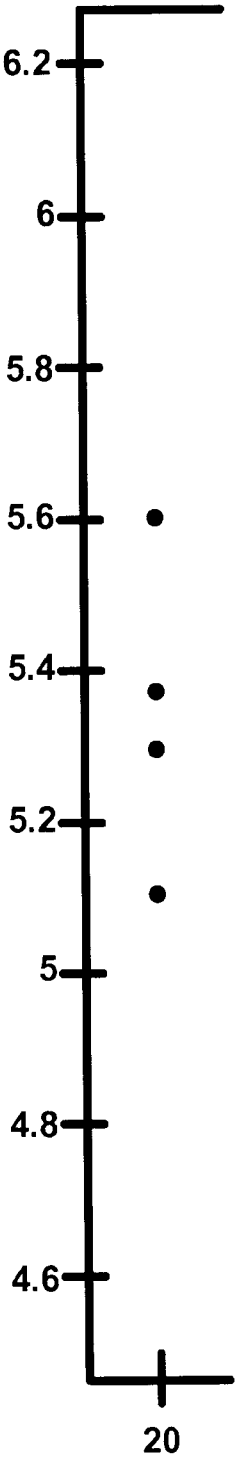


FIG. 2C

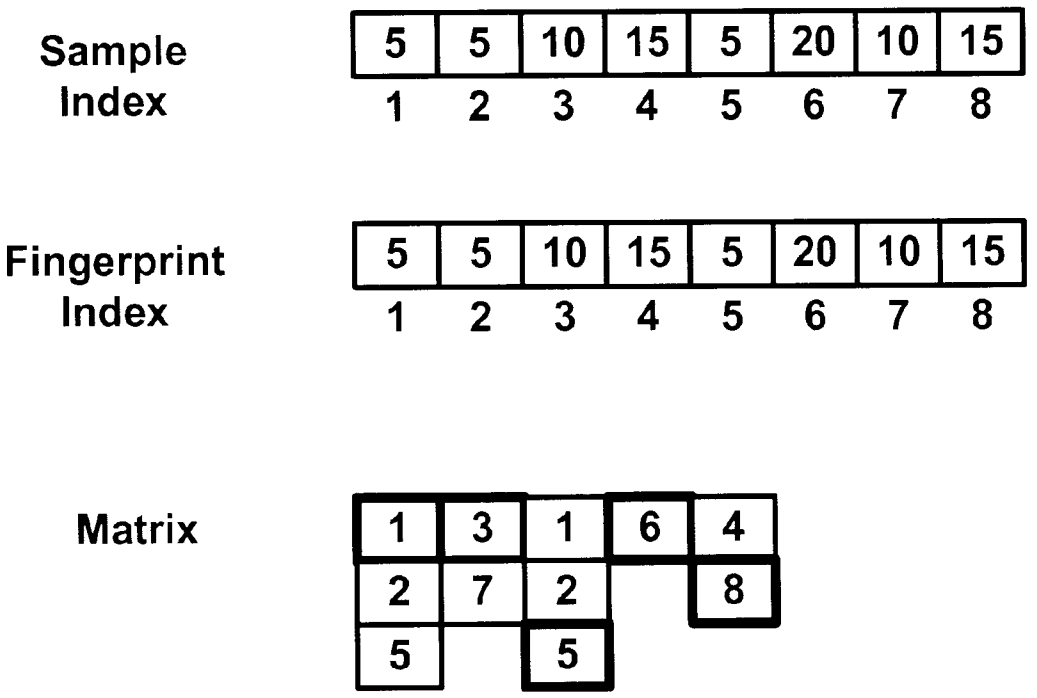

Sample Index
5 5 10 15 5 20 10 15
1 2 3 4 5 6 7 8
Fingerprint Index
5 5 10 15 5 20 10 15
1 2 3 4 5 6 7 8
Matrix
1 3 1 6 4
2 7 2 8
5 5

FIG. 3

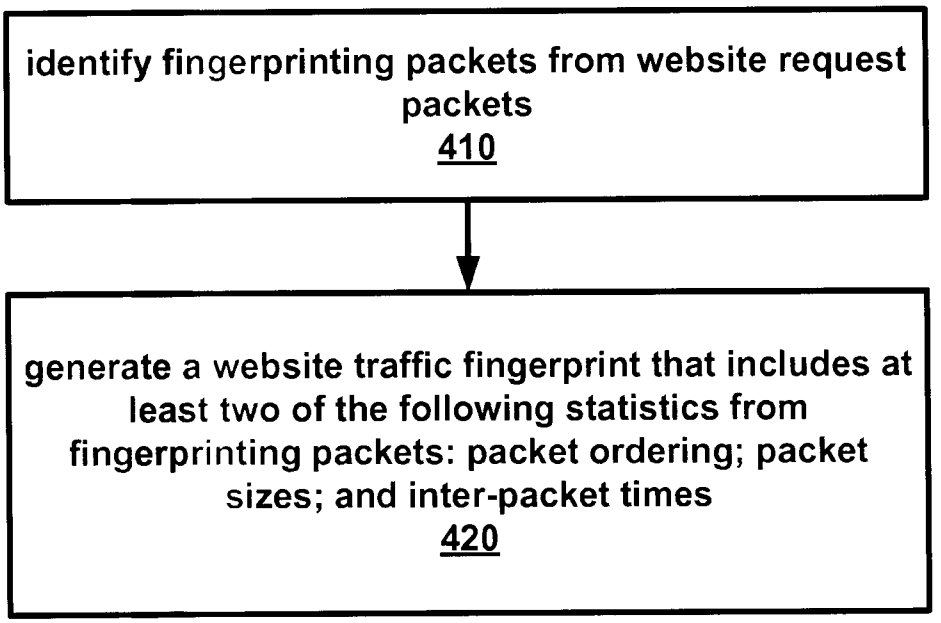

identify fingerprinting packets from website request packets
410
generate a website traffic fingerprint that includes at least two of the following statistics from fingerprinting packets: packet ordering; packet sizes; and inter-packet times
420

FIG. 4

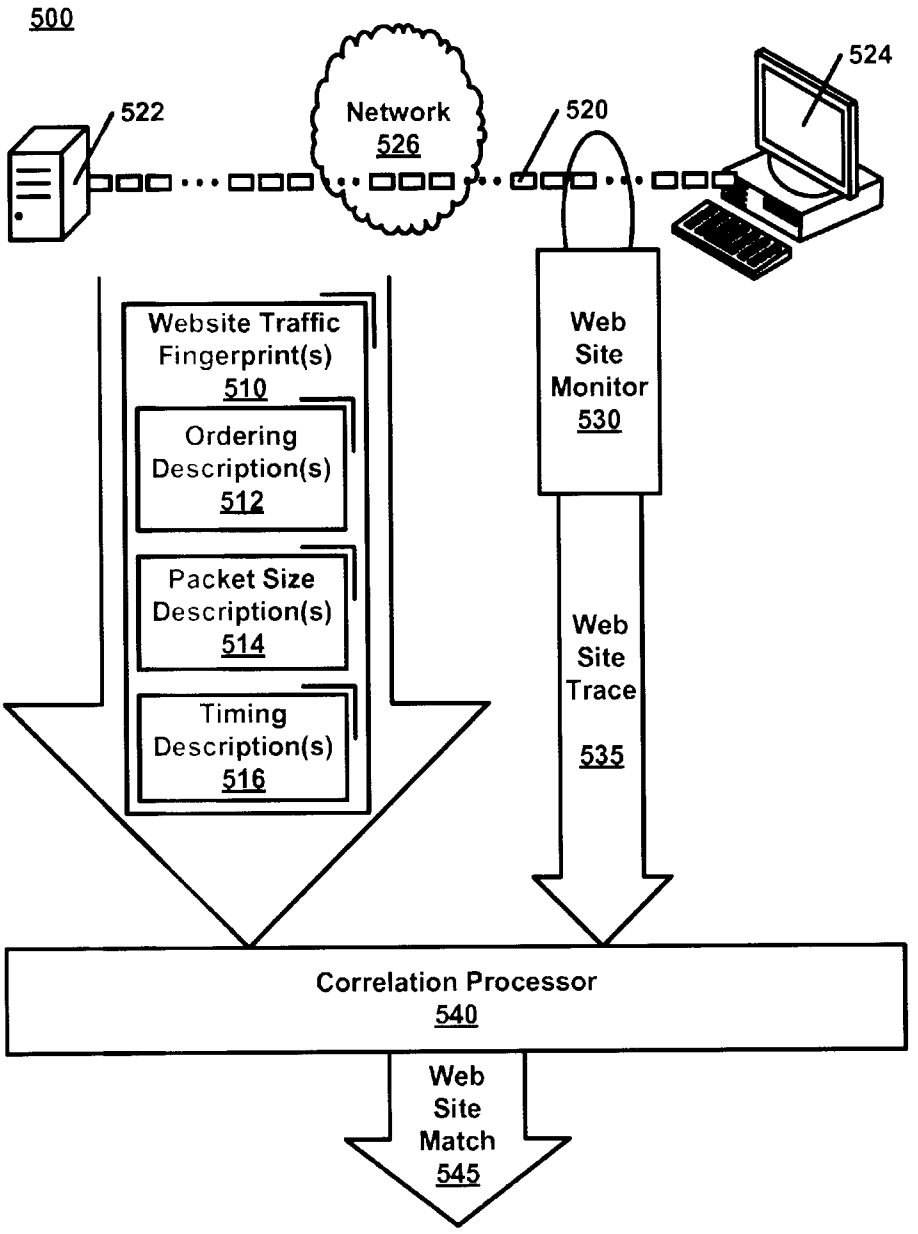

500
522
Network
526
520
524
Website Traffic
Fingerprint(s)
510
Ordering
Description(s)
512
Packet Size
Description(s)
514
Timing
Description(s)
516
Web
Site
Monitor
530
Web
Site
Trace
535
Correlation Processor
540
Web
Site
Match
545

FIG. 5

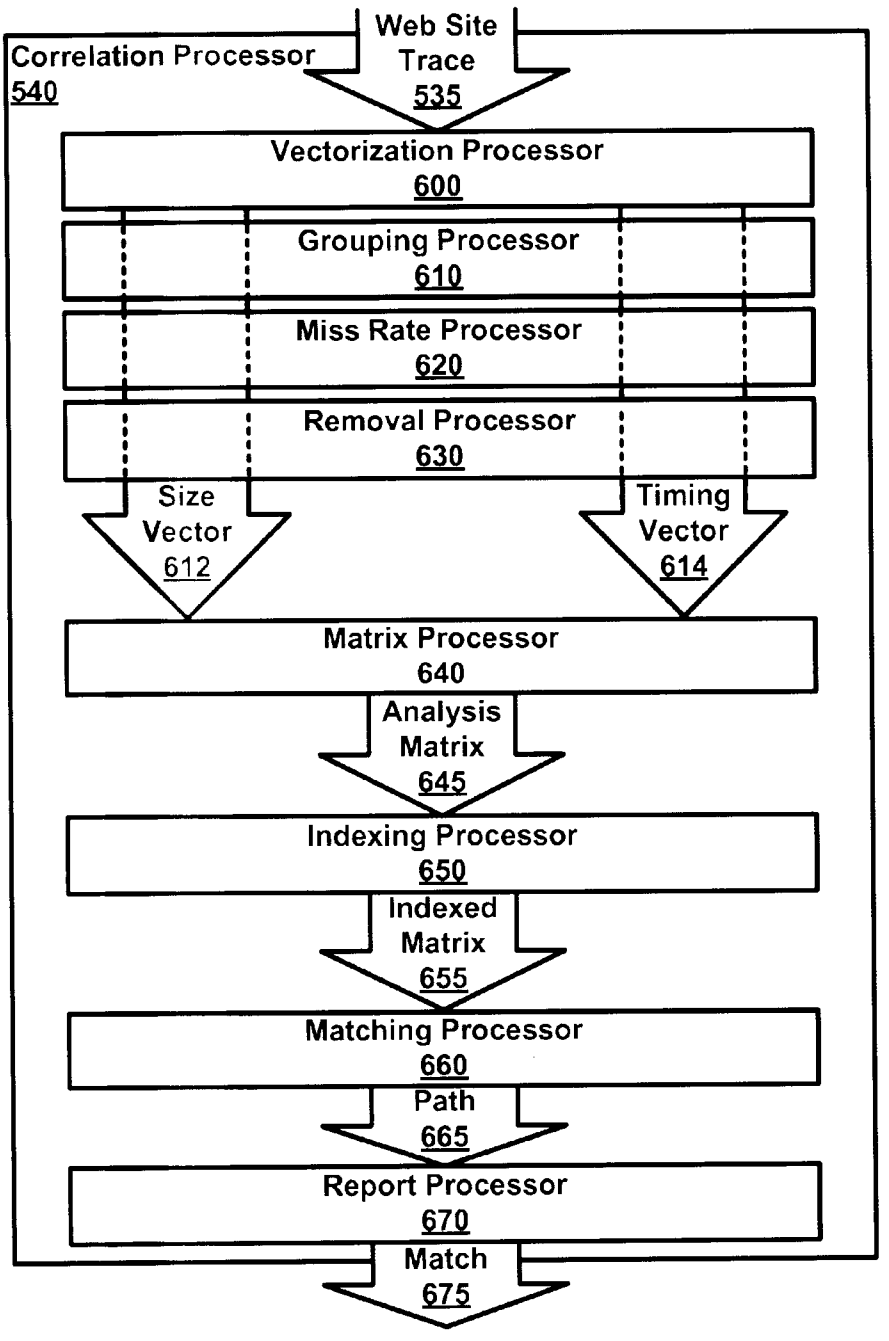

Correlation Processor
540
Web Site
Trace
535
Vectorization Processor
600
Grouping Processor
610
Miss Rate Processor
620
Removal Processor
630
Size
Vector
612
Timing
Vector
614
Matrix Processor
640
Analysis
Matrix
645
Indexing Processor
650
Indexed
Matrix
655
Matching Processor
660
Path
665
Report Processor
670
Match
675

FIG. 6

Doc ID: 6687066

WEBSITE MATCHING BASED ON NETWORK TRAFFIC

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 61/285,420, filed Dec. 10, 2009, entitled "Exposing Encrypted HTTP Traffic over VPN Using Pattern Learning," which is hereby incorporated by reference in its entirety.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

FIG. **1** is a plot showing a small sub-section of 100 packets from two separate web requests to different websites.

FIG. **2**A, FIG. **2**B and FIG. **2C** are graphs of minimum and maximum arrival times for website packets.

FIG. **3** is a diagram of an example matrix built from a sample set and a fingerprint as per an aspect of an embodiment of the present invention.

FIG. **4** is a flow diagram of process for generating a website fingerprint as per an aspect of an embodiment of the present invention.

FIG. **5** is a block diagram of a website detector **500** according to aspects of an embodiment of the invention.

FIG. **6** is an expanded block diagram of a correlation processor **540** according to an aspect of an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Embodiments of the present invention characterize network traffic associated with a website as a website traffic fingerprint that includes size, order, and timing statistics descriptive of packet traffic for the website. Further embodiments use the characterization to detect network traffic associated with that individual website regardless of: whether the packet data is encrypted or in the clear; and/or whether the packet data is mixed with other packet data.

Embodiments of the present invention determine information about web traffic inside a Virtual Private Network (VPN) tunnel. Specifically, some embodiments of the present invention search for fingerprints in encrypted traffic to enable determining information about web traffic inside a VPN tunnel.

A fingerprint in accordance with embodiments of the present invention includes data that characterize the communication of information to and/or from a website. In some embodiments, the data may include the size of packets, the ordering of packets and the timing of packets.

Embodiments may analyze multiple independent streams, and handle background noise or multiple sessions inside the same tunnel. Embodiments may also identify traffic from specific websites outside of VPN tunnels.

Virtual Private Networks, or VPN's, have become a common extension of many corporate and home networks. They allow disjointed entities to communicate in a very cost efficient manner, by using the Internet. Since this traffic can be very important to the users, the security of VPN's should be analyzed and well understood. In many cases, the algorithms used are very well tested and considered unreasonably difficult for an attacker to penetrate. Embodiments of the present invention analyze web traffic without attacking the encryption directly.

The usage of encryption to protect data provides confidentiality for data being sent through the tunnel. The inability to read data however, does not guarantee that something useful cannot be learned by analyzing a flow of data. For example, encrypting communications between two points does not hide the fact that communication is taking place, nor does it hide the amount of data that was transferred between the two points. Therefore, it may be important to understand what is protected when using a secure communication method. A lack of this type of understanding may be more dangerous than even an unsecured communication, as users may be working off a false assumption of anonymity.

The ability to use the characteristics of the transactions taking place across a VPN has provided multiple different areas of research. Using these techniques to analyze web traffic may reveal the source or destination of a communication. Patterns in the stream may be used to classify the type of traffic inside the tunnel. Similar data leakage may be used to analyze Voice over IP (VoIP) traffic to determine the language or recognize specific phrases. These are all examples of how the characteristics of an encrypted stream may still provide data.

According to embodiments, specifically in the case of analyzing Hypertext Transfer Protocol (HTTP) traffic, one may determine the websites visited under the assumption that only a single user's traffic is in the tunnel. Although some VPN's are intended for single users, it is also very common for VPN's to carry traffic of many users, or for a single user to produce additional traffic on the same link. In some cases, it may be difficult to separate out individual flows of data for traffic contained in the same tunnel. Embodiments of the present invention overcome this limitation.

A method that directly addresses the ability to analyze hypertext transfer protocol secure (https) traffic uses characteristics of the https protocol to assist in analyzing the captured flows. The main element used is the download of html pages, followed by overlapping requests for the remaining objects. The ability to discern this html file provides a means of fingerprinting websites. Further details might be gained by looking at the number and size of additional objects downloaded following the html section of the website. These can be categorized separately due to different source ports making the request for each object discernable even when multiple objects are being downloaded concurrently due to the https protocol encrypting each stream individually.

The ability to fingerprint websites based on the https protocol behavior inherently depends on the ability to separate out a single stream of traffic. As long a single user is making requests that do not overlap with other traffic, the workings of the protocol may be seen. When you apply additional requests or background traffic, this may become less clear. The assumption in these cases may be that html will never overlap with objects, due to the requirement that the html be fully downloaded before the objects are determined. However, if there are multiple browsing sessions included in the same tunnel, they could overlap making the size unrecognizable for either request.

In some cases, a setup may consist of a single user protecting http traffic with a secure shell (SSH) tunnel to a remote location. SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. According to embodiments, a third party may analyze sites by viewing the traffic between two encrypted endpoints. Profiles may be created for websites. Different statistical methods may be used for comparing the SSL traffic to the database of known and gathered characteristics.

Embodiments of the invention provide new mechanisms for analyzing a capture file. Assumptions that each individual request can be separated using timing may not be valid. Some embodiments overcome the assumption that html may need to be separated from objects. According to embodiments, determining these divisions may not be necessary to determine when a new website is visited. Some methods of comparison assume that only a single website exists in the captured comparison trace, and therefore may be compared to database of websites. Alternative embodiments handle multiple requests, background noise and multiple overlapping flows in the same tunnel.

According to embodiments, a database of the Internet (and parts thereof) could be created. This database might require volunteers profiling websites, and a modest amount of storage (e.g. 13 GB of storage). The feasibility of such a database is may be useful in multi-flow analysis that uses fingerprints of desired websites based on size and timing.

Embodiments may include: the ability to detect individual page loads based on the timing separation between pages, and the ability to detect TCP handshakes and closings by analyzing the size of the packets. In the case of a single user, all data during a page load may be compared to a fingerprint. According to embodiments, fingerprints may provide an ability to detect pages in the presence of background noise with complex matching.

Stream Analysis for Multiple Users

Useful information may be determined from encrypted traffic. However, embodiments may need to use packet characteristics in a way that is not flow dependent. Basically, embodiments may not assume that all packets from a single request are be grouped together. With this in mind, the following sections will discuss how embodiments may use packet size, timing, direction, and order to create flow independent website fingerprints.

Packet Size

To allow for packet size to remain relevant when multiple connections may overlap, the set of data that may overlap in a fingerprint may become more important. Fingerprints of a website may need to contain highly unique sizes, which indicates that not all packets may be relevant for a fingerprint. FIG. **1** is a plot showing a small sub-section of 100 packets from two separate web requests to different websites (netflix and newegg).

One observation is that many packets in these transactions are at one of the extremes of packet size. Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite that provides the service of exchanging data directly between two network hosts. TCP connections have a maximum packet size, and both transactions have many packets at this max. Secondly, TCP relies on acknowledgement packets, which comprise the bulk of the minimum packets seen in both transactions. These minimum and maximum packet sizes may provide very little information as to which website is actually being visited, since they may not be added all together. If these packets are included in a fingerprint, they are likely to increase false matches more than provide certainty of the intended website. In the case of the plot in FIG. **1**, only 20 packets out of the 100 shown were between the minimum and maximum packet sizes. Therefore up to 80% of this sub-section would match almost any other site if all packets were used.

Using this observation, embodiments may make a size portion of the fingerprints based on an "interesting" packet size range, which excludes maximum sized and minimum sized packets. The two traces in FIG. **1** are much more unique when only this section is viewed. This may provide a much more specific fingerprint and reduces false positives. Also, when every packet is not needed for a fingerprint, the effect of re-transmissions on detection can be reduced. Interesting packets may be defined as any packet above approximately 400 bytes and below approximately 750 to 1000 bytes. Interesting packets are also referred to as fingerprinting packets.

Timing and Order

A second available characteristic which carries through to the encrypted stream is the timing of the packets. Generally the round trip time of a packet is dependent on the location of the person accessing the server. This round trip time may not vary greatly between many sites, and requires the ability to associate a request with a response. Therefore a timing variable may be used which is both more unique per website, and not dependent on the ability to associate a specific request with a response.

To accommodate these restrictions, timing measurements between arrival times of interesting packets may be used. To correctly analyze timing in this way, a third characteristic of the traffic, the order of interesting packets, may be used. The interesting packet sizes should arrive in the same order for inter-arrival times to be relevant. The reduced number of packets due to limiting analysis to interesting traffic should make this possible. The accuracy of this process may rely on the arrival times between multiple sites to vary more than the round trip times mentioned earlier. To test this, interarrival time minimum and maximum timings for twenty similar websites were graphed. The minimum and maximum arrival times for each packet are graphed per website. FIG. **2**A shows the results for all websites, indicating that some websites have a very long range, and often would not match incorrect sites. FIG. **2**B shows a section of the 20th packet from all websites tested. Here it becomes clearer that min-max pairs have a distinct range. Finally FIG. **2**C shows a very small section of packets at the very bottom of the trace. These packets highlight that a very tight timing range can exist at any give point in the sequence. This tends to indicate that even if there is some over lapped timings for some sections of websites; it appears unlikely that the same website will contain overlapping timings for every interesting packet.

During fingerprint generation, the time between interesting packets may be recorded. These values may be stored for each pair; therefore 19 timing values may be needed with the fingerprint if there are twenty packets in the fingerprint. After multiple runs, the timing between each pair of packets may be analyzed to find a minimum and maximum arrival time for the website. Therefore, website fingerprints may consist of only interesting packets, in a specific order per website, with a set of timings between each packet.

Packet Direction

Another variable available with encrypted traffic is the direction of the traffic. Divide the stream into two directions, inbound and outbound. The inbound traffic would be all traffic arriving from the Internet towards the client, while the outbound traffic is the requests out from the client to the server. These two directions may be viewed as independent streams, since it may be difficult to reliably correlate requests to responses in a multi-user scenario. Comparing the inbound and outbound streams can provide two different observations.

First, the outbound packets may have a more reliable timing. The outbound packets may have very little network equipment to traverse before arriving at the monitoring point. The latency between the client and the VPN entry may therefore be low, when compared to latency times across the Internet. This low latency should create a more stable timing variation between packets. Additionally, requests from the client should not experience as much variance due to higher

load due to the simple nature of the request verses a server providing files and database access

Secondly, the outbound traffic may be more likely to arrive in the expected order as seen in the fingerprint. Again, a smaller amount of network equipment to traverse should decrease the chance of an out of order arrival. Additionally, the requests sent by the client are less likely to be broken up into unexpected sizes, while a server might provide some information differently according to its current load.

Due to these reasons, some embodiments may focus on attempting to detect websites in encrypted traffic based solely on the outbound stream of traffic. This may provide the additional benefit of reducing the number of packets which must be analyzed, as most web transactions have many more inbound packets than outbound.

The focus on outbound traffic could allow for one parameter defined earlier to be relaxed, the interesting packet size range. Inbound traffic has many maximum size packets, while outbound traffic has relatively few. Therefore, embodiments may re-define an interesting packet size to include these packets to obtain more fingerprint information, if only web traffic is present on the link to be analyzed. If, however, there may be other protocols on the link, a range may still be necessary since other protocols may result in large outbound packets. To ensure the method is more robust, embodiments may keep the range as defined earlier.

Multi-User Search Process

A detection mechanism may be utilizing using previously described metrics in a multi-flow environment. A website detector may be viewed as two subcomponents, the fingerprint generation mechanism, and the comparison mechanism. The fingerprint mechanism may be provided with many samples of a web request, and subsequently generate website fingerprints. The comparison mechanism may be provided a trace file to be analyzed and website fingerprints for sites to be identified. The comparison mechanism may then determine if any sequences in the trace match the provided fingerprints and return the results. The following sections will describe how these two mechanism work.

Fingerprint Generation.

To generate a fingerprint, trace files of successful visits to the websites to be fingerprinted should be collected. In some embodiments, it may be advantageous that the only traffic in the trace belongs to the desired website. Fingerprint generation may require a large number of traces to ensure the fingerprint can accurately reflect the site under varying conditions.

As an example, this information may be gathered using two Linux machines, with an OpenVPN connection between them. One end would be the "client" end of the connection, while the other would run a web proxy listening locally on the tunnel interface. The client may make web requests through the tunnel to the proxy server on the other side. Using tcpdump, capture files may be created of both the clear text, and encrypted traffic, at the same time. Having both traces allows for using the encrypted traffic for fingerprint generation, while still maintaining the clear text to analyze any unexpected behavior. This process may be scripted. In an example test, this process was run to gather 100 traces for each website to be analyzed. Once the capture files are available, a fingerprint may be made for each site.

Example traces for a specific site may be made accessible to the fingerprint generation mechanism. Each trace may be divided into the inbound and outbound directions. As described earlier, some embodiments may only focus on the outbound direction traffic. Foe the purposes of describing this particular embodiment, in the remaining steps only the outbound traffic is used. Additionally, embodiments may focus only on the interesting, as defined earlier, from each of these traces.

Trace files which contain packets with the correct direction and size may be analyzed. Traces may be analyzed and a pair of vectors created to describe each trace. The first vector may contain the size of each packet, in the order they are seen in the trace file. The second vector may contain the time at which each packet arrived. The length of the vectors may depend on the number of interesting packets in the corresponding trace file they were generated from. Since the index may represent the order of the packets, these two vectors may quickly allow the determination of arrival time and size of packets according to their order of arrival. The two vectors may need to be keep consistent, therefore any alterations or deletions may need to be completed on both vectors the same way.

Once the vectors are created for test runs of a site, vectors may be grouped together by vector length. These groupings may represent multiple possible sub-fingerprints for a single website. Since timing may be defined as the difference since the last interesting packet, the number of interesting packets may have a large impact. Therefore these sub-fingerprints may allow for some variation in expected responses while keeping the timing data a viable means of comparison.

Each of these groupings may now undergo processing to create website fingerprint(s). The processing may accomplish two goals. First, network errors or anomalies may be removed from test sets. Fingerprint generation may be automated to allow for large number of runs. However, a mechanism may be necessary to ensure that any errors in page loads or network problems do not corrupt fingerprint(s). A first step may be to remove detectable errors to ensure a clean fingerprint(s). After this process, there may still be some variation due to a website itself. For example, there might be some page loads which are requested in slightly different order, which is common for the page. Therefore, it may be useful to reduce the sub-fingerprints of group(s) down to similar portions of a requests while still keeping the fingerprint unique enough to match.

According to embodiments, one reduction reduction may focus on removing vectors that fall into these groups, but are very far apart from any other vectors. These may be detected by finding a "miss rate" for vector(s) in the group. To find this, embodiments may start with the first element of the vector to be tested, and compare its size value to all other vectors in the same group. A miss may be recorded for every mismatch found. This may be done for every element of the vector to be tested, resulting in a miss rate for the entire vector. This miss rate may then be used in formula (1) to generate a miss ratio. The number of misses is represented by m. The number of elements in the current group is represented by g. The length of the vectors in the group is represented by l

$$(m\ g)\ l \tag{1}$$

Vectors containing a very high miss ratio may represent data which is most likely bad, but still happened to be of the correct length to fit into the group. Any vectors that have a miss ratio over a set threshold may be removed from the group, as they may represent errors that could corrupt the fingerprint.

According to embodiments, another reduction may focus on correcting for small variations which may be common due to factors such as dynamic web content, adds on to a page, etc. These might still generate the same number of requests, but it is possible that some get requests could be a slightly different size, causing the vectors to not match every size exactly the same. To generate a single fingerprint representing the entire

group, while still allowing for these variations, embodiments may remove the variable packets from the fingerprints. The first index in the first vector may be compared to the first index of every other vector in the group. If the index is not found to match every other vector in the group, then that index may be removed from all vectors in the group. This may be repeated for every index in the vector, removing any that do not match all other vectors in the group. When done, the remaining vectors may all match, in size and sequence. The removed entries may represent the variable data from the website, while the remaining entries may be the data point which should always be present. The remaining vector may provide the size-order portion of the fingerprint for the group.

Additionally, the number of traces in each grouping may be evaluated and any grouping with less than a minimum number of traces dropped. These groups may still be present especially if they contain only a single element. A single element group may not have been removed by the previous methods as they may not have any error rate at all, but still represents data which needs to be removed.

Finally, the timing portion of the fingerprint may be created for the groups. Each vector in a group may have corresponding timing vectors, which have been altered in the same way as the size vectors. To create a timing vector, the first and second entries may be compared to find the time delay between these two interesting packets. This may be done for all vectors in the group, and the minimum and maximum delays seen may be recorded for the timing portion of the fingerprint. This may be done for each interesting packet pair in the sequence, resulting in a minimum and maximum expected inter-arrival time for all packets in the sequence.

According to embodiments, the timing data, along with the size-order data, creates one sub-fingerprint for the designated website. A website may contain multiple sub-fingerprints, one for each grouping found. All sub-fingerprints together may create a fingerprint for the website as a whole. When testing for a match, any of these sub-fingerprints being found may indicate a match for the website.

Comparison Mechanism

The previous sections describe how to generate fingerprints for sites to be tested. Once these fingerprints are available, captured network traffic may be searched for a matching fingerprint. For this, embodiments may use a comparison mechanism designed to look for the qualities provided in the fingerprints. To accomplish this, the captured packet data may be formatted, a search matrix constructed, and the matrix traversed to determine if a matching path exists. The following paragraphs describe embodiments of this process.

First, a data stream to be tested may be captured in a trace file. For some embodiments, rather than requiring processing to filter out the inbound data, only outbound data needs to be captured. This data may be made available to a matching mechanism that may generate size vector(s) and timing vector (s) as was done for the fingerprints. According to embodiments, these two vectors may contain only data which falls into the interesting range as defined previously, reducing the size of the required matrix and ignoring traffic which will never match the fingerprint. The resulting data may be in a similar format to the fingerprints, although many different flows may be present from multiple web requests.

According to embodiments, after formatting the input data, a matching mechanism may create an analysis matrix that may be used to find possible matches. When looking for matches, a single sub-fingerprint from the websites combined fingerprint may be analyzed at a time. The matrix may contain a column for each entry in the fingerprint being analyzed. Each column may contains index references to packets that match the required size for the fingerprint. The vector containing the traffic to be analyzed may be traversed, comparing the size of the packet at the current index, to all indexes of the fingerprints size vector. Every time a matching size is found, the index of the test set may be recorded in the corresponding column in the analysis matrix. It is possible that a single packet size is found in multiple locations in the fingerprint, and therefore any packet in the analysis trace may be recorded in multiple columns in the matrix.

FIG. **3** shows an example matrix built from a sample set and a fingerprint. In this example, the sample and fingerprint rows represent size values, while the index is for easy reference to the location in the vector. Each column of the matrix contains all indexes where the fingerprints required size is matched. Since the fingerprint has the same size for the first and third packets, these columns in the matrix are identical. The sample is traversed, and all matching sizes have their index stored in the matrix, as shown.

Once the matrix has been generated, the matching process may then determine if an acceptable path exists through the matrix. The matrix may provide all packets of the appropriate size, but it may also be checked against the timing requirements from the fingerprint. Embodiments start with the first entry in the first column of the analysis matrix. This is the first packet that matches the correct starting size for the fingerprint. The index of this packet allows the arrival time to be quickly referenced. The arrival time of the first packet in the second column may be also determined. The difference in these arrival times may then be compared to a minimum and maximum time range of the fingerprint. If the time is not within the range, the next entry in the second column may be checked until a match is found or no other entries are available. If no matches are found, the process may start over again with the second entry in the first column, again searching for any timing that is within the range specified in the fingerprint. If a match is found, the columns in the search may be advanced, and the matching packet used as the new starting point, and the third column may be searched for an acceptable timing value. If a complete path is found through the matrix, then there exists a sequence of packets which match the given fingerprint size, order, and timing.

In the previous example shown in FIG. **3**, one possible path through the matrix is indicated as bold boxes. This path may assume the timing of these packets were within the acceptable range. If they were not, an alternate path could have stated with the second entry in the first column.

This process may be done for each sub-fingerprint of a given website to look for all known variations of traffic associated with the given site. If a match is found, it is possible to not only return a result but to provide the packet sizes in the trace as well as the exact timing for the detected sequence.

FIG. **4** is a flow diagram of process for generating a website fingerprint. This process may be computer implemented using one or more computing machines. Embodiments of the process (or parts thereof) may be substantiated on one or more non-transient tangible computer readable mediums that contain computer readable instructions that when executed by one or more processors, causes the one or more processors to execute all or part of the process. Examples of non-transient tangible computer readable mediums include: solid-state memory, flash drives, hard drives, floppy drives, optical disks, DVDs, CDs, Blu-ray discs, or the like.

At **410**, fingerprinting packets from website request packets to a website may be identified. The identification of fingerprinting packets may include looking at the packet size of each packet. Packets that have a size that is less than a minimum packet size may be rejected. A typical minimum packet

size may be approximately 400 bytes. Similarly, packets that have a size that is greater than the maximum packet size may also be rejected. A typical maximum packet size may be approximately 1000 bytes. One of the features of some embodiments is that fingerprinting packet(s) may be encrypted.

Each of the fingerprinting packet(s) may also have a temporal location within the website requests. The temporal location is the location within the sequence of packets comprising a website request. Often, the temporal location may be described using a timestamp. Timestamp(s) may be internal to fingerprinting packet(s) or derived from an arrival time measurement of the fingerprinting packet(s).

Website traffic fingerprint(s) may be generated at **420**. Website traffic fingerprint(s) may include: an ordering description, a size description, a timing description, or a combination thereof. The ordering description may include ordering data of at least two of the fingerprinting packets determined using the temporal location for each of the at least two of the fingerprinting packets. The size description may include size data of the packet size of at least two of the fingerprinting packets. The timing description may include timing data of at least two inter-packet times for at least two of the fingerprinting packets determined using the temporal location for each of the at least two of the fingerprinting packets; or a combination thereof. The ordering and the inter-packet times may be determined using the same fingerprinting packets.

FIG. **5** is a block diagram of a website detector **500** according to aspects of an embodiment of the invention. Computer **524** is communicating with a Web server **522** via website packet flow **520** through network **526**.

Web site monitor **530** may be configured to generate at least one web site trace **535** of packet statistics related to fingerprinting packets from website packet flow **520**. Website packet flow **520** may be encrypted. Fingerprinting packets may be a subset of the website packet flow **520** having a packet size between a minimum packet size and a maximum packet size. A typical minimum packet size may be approximately 400 bytes and a typical maximum packet size may be approximately 1000 bytes.

The website detector **500** uses website traffic fingerprint(s) **510** that describe the website packet flow **520** for specific websites. Website traffic fingerprint(s) may include: an ordering description(s) **512**, a size description(s) **514**, a timing description(s) **516**, or a combination thereof. The ordering description(s) **512** describes the temporal order of fingerprinting packet(s). The packet size description(s) **514** describe size of fingerprinting packet(s). The timing description(s) **516** describes inter-packet times between pairs of fingerprinting packet(s).

A correlation processor **540** may be configured to correlate a sequence of packet statistic(s) from the web site trace **535** with the size description(s) **512**, the order description(s) **514**, and timing description(s) **516** found in website traffic fingerprint(s) **510**. Correlation processor **540** outputs any matches **545** between the web site trace **535** and website traffic fingerprint(s) **510**.

FIG. **6** is an expanded block diagram of a correlation processor **540** according to an aspect of an embodiment of the present invention. As shown, the correlation processor **540** includes a vectorization processor **600** configured to use the web site trace **535** to create size vector **612** and timing vector **614**. Size vector **612** may include ordered size statistics about fingerprinting packets and timing vector **614** may includes temporal information about fingerprinting packets. According to embodiments, size vector **612** and timing vector **614** may need to be kept consistent, especially when processed. According to some embodiments, the web site trace **535** may limit the statistics to fingerprinting packets in the outbound direction.

According to embodiments, grouping module **610** may be implemented in embodiments of the correlation processor **540**. The grouping module **610** may be configured to group size vector entries and timing vector entries by at least one characteristic. These grouping could be treated as a sub-fingerprints. Characteristics may include any type of information useful in describing an embodiment relevant characteristic of a fingerprinting packet such as the length of a fingerprinting packet, an association of the fingerprinting packet with particular portions of web site requests, etc.

According to embodiments, miss rate processor **620** may be implemented in embodiments of the correlation processor **540**. Miss rate processor **620** may be configured to calculate a miss rate among vectors in a grouping. A miss occurs when the length of a vector falls outside a prescribed limit. The number of misses is used to calculate a miss rate ratio. The miss rate processor **620** may remove variable packet vector(s) whose miss rate ratio exceeds a miss rate threshold from a grouping.

According to embodiments, removal processor **630** may be implemented in embodiments of the correlation processor **540**. Size vector entries and timing vector entries associated with network errors or anomalies may corrupt a website fingerprint. Removal processor **630** may be configured to remove these size vector entries and timing vector entries associated with network errors or anomalies.

According to embodiments, matrix processor **640** may be implemented in embodiments of the correlation processor **540**. Matrix processor **640** may be configured to create an analysis matrix **645** using the size vector **612** and the timing vector **614**.

According to embodiments, indexing processor **650** may be implemented in embodiments of the correlation processor **540**. Indexing processor **650** may be configured to generate an indexed matrix **655** by indexing index size vector entries **612** in the analysis matrix **645** to fingerprint size vector entries that have sizes that are within an configurable error margin.

According to embodiments, matching processor **660** may be implemented in embodiments of the correlation processor **540**. Matching processor **660** may be configured to determine if a path **665** exists through the indexed analysis matrix **655**. The matching processor **660** may attempt to locate a path through the indexed analysis matrix **655** by sequentially matching the inter-packet times between indexed entries in the indexed analysis matrix **655**.

According to embodiments, reporting processor **670** may be implemented in embodiments of the correlation processor **540**. Reporting processor **670** may be configured to output a positive indicator **675** when the matching processor **660** determines that a path **665** exists through the indexed analysis matrix **655**.

Additional website request information about a website could improve a website fingerprint. Packet statistics from web site trace(s) **535** may be used to update website traffic fingerprint(s).

In this specification, "a" and "an" and similar phrases are to be interpreted as "at least one" and "one or more."

Many of the elements described in the disclosed embodiments may be implemented as modules. A module is defined here as an isolatable element that performs a defined function and has a defined interface to other elements. The modules described in this disclosure may be implemented in hardware,

a combination of hardware and software, firmware, wetware (i.e hardware with a biological element) or a combination thereof, all of which are behaviorally equivalent. For example, modules may be implemented as a software routine written in a computer language (such as C, C++, Fortran, Java, Basic, Matlab or the like) or a modeling/simulation program such as Simulink, Stateflow, GNU Octave, or LabVIEW MathScript. Additionally, it may be possible to implement modules using physical hardware that incorporates discrete or programmable analog, digital and/or quantum hardware. Examples of programmable hardware include: computers, microcontrollers, microprocessors, application-specific integrated circuits (ASICs); field programmable gate arrays (FPGAs); and complex programmable logic devices (CPLDs). Computers, microcontrollers and microprocessors are programmed using languages such as assembly, C, C++ or the like. FPGAs, ASICs and CPLDs are often programmed using hardware description languages (HDL) such as VHSIC hardware description language (VHDL) or Verilog that configure connections between internal hardware modules with lesser functionality on a programmable device. Finally, it needs to be emphasized that the above mentioned technologies are often used in combination to achieve the result of a functional module.

The disclosure of this patent document incorporates material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, for the limited purposes required by law, but otherwise reserves all copyright rights whatsoever.

While various embodiments have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art(s) that various changes in form and detail can be made therein without departing from the spirit and scope. In fact, after reading the above description, it will be apparent to one skilled in the relevant art(s) how to implement alternative embodiments. Thus, the present embodiments should not be limited by any of the above described exemplary embodiments. In particular, it should be noted that, for example purposes, the above explanation has focused on the example(s) analyzing website traffic. However, one skilled in the art will recognize that embodiments of the invention could be used to analyze other types of packet traffic related to other types of communications such as communications to mail servers, DNS servers, ftp severs, peer to peer communications, SCADA communications, etc.

In addition, it should be understood that any figures that highlight the functionality and advantages, are presented for example purposes only. The disclosed architecture is sufficiently flexible and configurable, such that it may be utilized in ways other than that shown. For example, the steps listed in any flowchart may be re-ordered or only optionally used in some embodiments.

Further, the purpose of the Abstract of the Disclosure is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientists, engineers and practitioners in the art who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The Abstract of the Disclosure is not intended to be limiting as to the scope in any way.

Finally, it is the applicant's intent that only claims that include the express language "means for" or "step for" be interpreted under 35 U.S.C. 112, paragraph 6. Claims that do not expressly include the phrase "means for" or "step for" are not to be interpreted under 35 U.S.C. 112, paragraph 6.

What is claimed is:

1. A computer implemented process comprising:

identifying fingerprinting packets from website request packets to a website, at least one of the fingerprinting packets being encrypted, each of the fingerprinting packets having:

a packet size between a minimum packet size and a maximum packet size; and

a temporal location within the website requests; and

generating a website traffic fingerprint that includes at least two of the following:

an ordering description of at least two of the fingerprinting packets determined using the temporal location for each of the at least two of the fingerprinting packets:

a packet size description of at least two of the fingerprinting packets; and

a timing description of at least two inter-packet times for at least two of the fingerprinting packets determined using the temporal location for each of the at least two of the fingerprinting packets.

2. The computer implemented process according to claim 1, wherein the temporal location is determined using a timestamp.

3. The computer implemented process according to claim 2, wherein the timestamp is internal to at least one of the fingerprinting packets.

4. The computer implemented process according to claim 2, wherein the timestamp is derived from an arrival time measurement of at least one of the fingerprinting packets.

5. The computer implemented process according to claim 1, wherein the minimum packet size is less than 400 bytes.

6. The computer implemented process according to claim 1, wherein the maximum packet size is greater than 1000 bytes.

7. The computer implemented process according to claim 1, wherein the ordering and the inter-packet times are determined using the same fingerprinting packets.

8. A website detector comprising:

a module configured to receive at least one website traffic fingerprint that includes at least one of the following:

an ordering description of at least two fingerprinting packets;

a packet size description of at least two of the fingerprinting packets; and

a timing description of at least two of the fingerprinting packets; and

a website monitor configured to generate at least one website trace of packet statistics related to fingerprinting packets from a website packet flow, at least one of the fingerprinting packets being encrypted, each of the fingerprinting packets having a packet size between a minimum packet size and a maximum packet size; and

a correlation processor configured to correlate a sequence of packet statistics in at the at least one website trace with the size description, the order description, and timing description found in at least one of the at least one website traffic fingerprints.

9. The website detector according to claim 8, wherein the correlation processor includes a vectorization processor configured to use the website trace to create:

a size vector that includes ordered size statistics about fingerprinting packets; and

a timing vector that includes temporal information about fingerprinting packets.

10. The website detector according to claim 9, wherein the size vector and timing vector are kept consistent.

11. The website detector according to claim 9, further including a grouping module configured to group size vector entries and timing vector entries by at least one characteristic.

12. The website detector according to claim 11, wherein at least one characteristic is length.

13. The website detector according to claim 11, wherein at least one characteristic is an association with similar portions of website requests.

14. The website detector according to claim 11, further including a miss rate processor configured to calculate a miss rate among vectors in a grouping.

15. The website detector according to claim 14, wherein the miss rate processor is further configured to remove variable packet vectors whose miss rate ratio exceeds a miss rate threshold from a grouping.

16. The website detector according to claim 9, further including a removal processor configured to remove size vector entries and timing vector entries associated with network errors or anomalies.

17. The website detector according to claim 9, further including a matrix processor configured to create an analysis matrix using the size vector and the timing vector.

18. The website detector according to claim 17, further including an indexing processor configured to index size vector entries in the analysis matrix to fingerprint size vector entries that have sizes that are within a configurable error margin.

19. The website detector according to claim 18, further including a matching processor configured to determine if a path exists through the analysis matrix.

20. The website detector according to claim 19, wherein the matching processor is configured to locate the path through the analysis matrix by sequentially matching the inter-packet times between indexed entries in the analysis matrix.

21. The website detector according to claim 19, further including a reporting processor configured to output a positive indicator when the matching processor determines that the path exists through the analysis matrix.

22. The website detector according to claim 8, wherein the website trace includes at least one statistic related to fingerprinting packets in the outbound direction.

23. The website detector according to claim 8, wherein at least one packet statistic from at least one website trace is used to update at least one website traffic fingerprint.

* * * * *

Doc ID: 6687067

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Gathering Information
Date: Sunday, September 21, 2014 1:59:33 PM

Can you please give me information about the National Security Agency – Technology Transfer Program? I would prefer to know every detail you can give and more information about the Computer & Information Sciences Researcl
because I could find no contact detail of someone who can provide the information I like to know and do not forget to give the information I like to know about the Technology Transfer Program too.

[redacted]

Doc ID: 6687069

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Retrieving Electronic Data During Enhanced Note Taking
Date: Thursday, January 09, 2014 1:36:27 PM
Attachments: NSA.Tech.Transfer retreiving data.pdf

As a follow up, INADEV sent a written request to the NSA Technology Transfer Program a couple of months ago regarding the above-referenced patent (summary sheet attached). I would like to speak with someone regarding the potential transfer of this patent as soon as possible. My contact information is below. Thanks.

[redacted]
Chief Executive Officer

(b) (6)

[redacted]

1651 Old Meadow Rd., Suite 205
McLean, Virginia 22102
www.inadev.com

[redacted]

Technology Profile Fact Sheet

Title: Retrieving Electronic Data during Enhanced Note Taking

Aliases: None

Technical Challenge: To search and retrieve data while taking handwritten notes.

Description: This invention gives a person taking handwritten notes the ability to search and retrieve data contained in computerized data bases in near real time. This invention gives the note taker the additional ability to delineate specific terms while taking notes while requesting general or specific additional information. The invention combines several existing technologies -- such as any of the existing "smart pad" technologies -- to automatically capture and extract information and instructions from written notes while connecting computer data sources with the note taker's display through wireless technology.

Demonstration Capability: Sketches of the physical layout with a process description are available. Individual technologies can be displayed separately.

Potential Commercial Application(s): There is large potential for use in differing markets where easy ad hoc data entry and retrieval with key-word customization is needed. These diverse markets might include critical areas such as law enforcement and public safety, customer and sales oriented activities such as Customer Relationship Management (CRM) and Sales Force Automation (SFA), warehouse management systems (WMS), or supply and distribution chain management.

Patent Status: Patent application has been filed with USPTO.

Reference Number: 1513

Doc ID: 6687070

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: short visit
Date: Thursday, November 06, 2014 3:05:38 PM

Dear Sir or Madam.

I would like to have a short visit with someone from the tech transfer office to discuss technology transfers. I have a badge and could meet wherever you designated.

Thank you for your attention to this request.

[redacted] (b) (6)

--
[redacted]
Director-Strategic Initiatives
Amches, Inc.
[redacted]

Doc ID: 6687071

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: Tamper Indicating Label
Date: Friday, August 22, 2014 4:19:17 PM

Greetings TTP,

Requesting assistance in obtaining Tamper Indicating Labels and Reusable Tamper Indicating Security Devices from NSA for use on classified hard drives.

Sincerely,

(b) (6)

[redacted]
Information Security Specialist
Army Sustainment Command: G2
AMSAS-IN
Rock Island Arsenal, IL
[redacted]

[redacted]

Doc ID: 6687072

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Ttsa
Date: Tuesday, August 12, 2014 1:23:47 PM

Hello.
I work at NASA/ARC. as a support contractor with their small satellite projects, and would be interested in obtaining more information on your wide band retro reflector listed in your 2014 tech transfer file.
Thanks

[redacted] (b) (6)

Sent from my iPad

[redacted]

Doc ID: 6687073

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Technology Transfer
Date: Monday, October 06, 2014 6:55:45 PM

Hello

I am with the Department of Defense and I am the technology manager for a pilot project that establishes the continuous evaluation of cleared personnel. I saw several interesting excerpts about technology the NSA has for doing context relevant searching of data to determine relationships of data.

I would like to know if the DoD is eligible to participate in this program or if there is another for intergovernmental transfers.

(b) (6)

Regards,

[redacted]
Program Manager DBIDS

[redacted]
Defense Manpower Data Center (DMDC)
Office 8000, 400 Gigling rd., seaside CA 93955

DMDC is on Facebook and Twitter! Check us out...
- http://www.facebook.com/go2dmdc
- http://www.twitter.com/dmdc

[redacted]

Doc ID: 6687074

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: CRADA Program
Date: Thursday, November 19, 2015 10:30:18 PM

As a private citizen, without a business of my own, nor being a member of academia, is there still an avenue available to me via CRADA for tech. transfer?

I have a large collection of design concepts with wide-ranging applications and implications to homeland security.

I am looking to share these designs for immediate development with the NSA, as I know they may have a direct impact on HUMINT, SIGINT, IA, and other high priority needs.

Thank you.

[redacted]

(b) (6)

[redacted]

Doc ID: 6687075

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: FBI Software Inquiry
Date: Tuesday, March 31, 2015 2:40:16 PM

(b) (6)

Hello,

My name is [redacted] I'm a Computer Scientist here at the FBI. One of my associates at the FBI here was told me that this would be the correct e-mail to contact regarding obtaining a piece of software known as "ghidra". Could you please point me in the right direction?

Thanks!

(b) (6)

[redacted]
Boston FBI,
Computer Scientist

[redacted]

Doc ID: 6687076

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: from wall street journal - comment on onyara acquisition
Date: Tuesday, August 25, 2015 6:53:31 PM

Hi there,
I cover technology in the Wall Street Journal's San Francisco bureau. I saw that Onyara Inc was acquired. I'd like to get some background on the technology transfer program, which I wasn't familiar with until now. When was it launched? Can someone chat about the origin of the technology transfer program?

Many thanks,

(b) (6)

[redacted]
Reporter
The Wall Street Journal
[redacted]

[redacted]

Doc ID: 6687077

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: National Security Agency – Technology Transfer Program
Date: Tuesday, March 03, 2015 2:34:36 PM

Greetings,

I recently created a service-disabled, minority owned small business (Cyber Research and Intelligent Solutions Provider--CRISP) which focuses on various "disruptive technologies." Basically, my company actively pursues the SBIR/STTR Grant opportunities (http://www.sbir.gov/about/about-sttr) as well as cyber security related consulting. Since CRISP has various strategic partners, which provides various types of expertise, I would like to enter into the NSA's Technology Transfer Program. Thanks in advance for your time and I look forward to your reply.

(b) (6)

Respectfully,

[redacted] Founder and CEO, Cyber Research and Intelligent Solutions Provider (CRISP)
www.crisp-llc.com
[redacted]

Approved for [redacted]

Doc ID: 6687078

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Interested in Data Port Protection Products
Date: Wednesday, August 19, 2015 11:47:22 AM

Hi,

I recently attended the IAS Conference and received material about USB and Data Port Protection products that you are developing. We have determined that the RJ45 (Ethernet) Port Protector would fit one of our current needs perfectly. On the brochure it states that samples are available, would we be able to get some samples so that I could show this off as a potential solution? If we go ahead with this as the solution, how would we purchase them? Thanks in advance for your help.

Thanks,

(b) (6)

[redacted]
Information Assurance Specialist
Cyber Security Operations, Org. 00097
Sandia National Laboratories, MS 1202

[redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: NC State University IP
Date: Tuesday, August 18, 2015 12:21:23 PM

To whom it may concern.

I am from the Tech Transfer office at North Carolina State University. We have received an invention disclosure in our office that had NSA funding through our Laboratory of Analytic Sciences.

Under the Bayh-Dole Act, we are required to notify the federal agency of any such subject invention. Typically I do this through iEdison, but NSA does not seem to be an agency that uses that interface.

Would you please direct me to the person who I should notify?

Thank you,

(b) (6)

[redacted]

--

[redacted] MLIS
Assistant Director, Operations & Strategy
Office of Technology Transfer
North Carolina State University
1021 Main Campus Drive
Campus Box 8210
Raleigh, NC 27695
[redacted]

No trees were killed in the sending of this message but a large number of electrons were terribly inconvenienced.

technology=15263

Approved for [redacted]

Doc ID: 6687080

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: Notification to DOD.NSA re: Government Waiver of Rights
Date: Monday, June 01, 2015 10:51:43 AM
Attachments: 2013-058 Notification to DOD.NSA re.Government Waiver of Rights.docx.pdf

Please see attached letter waiving to Government all rights in invention 2013-058.

(b) (6)

[redacted]
Office of Innovation Advancement and Commercialization
570 Devall Drive, Ste. 102
Auburn, AL 36832
[redacted]

[redacted]

Doc ID: 6687080

AUBURN UNIVERSITY

OFFICE OF IN VATION ADVANCEMENT AND COMMERCIALIZATION

June 1, 2015

National Security Agency Technology Transfer Program
Via email:tech_transfer@nsa.gov
9800 Savage Road, Suite 6848
Ft. Meade, MD 20755-6848

RE: DOD/NSA Contract/Grant No.: H98230-12-C-1102-1AF (b) (6)
PI – [redacted]

AU Invention No.: 2013-058 "Micromachined Rare Earth Magnet DC Current Sensor"
Disclosure Date: 6/24/2013 (Previously reported via USPS)

To Whom it May Concern:

Pursuant to the above-referenced contract/grant notification of the invention previously reported, please note that Auburn University waives to Government all rights in the referenced invention on this date and will take no further action in this matter.

Please feel free to contact our office with any questions or concerns you may have.

Best regards,

[redacted] (b) (6)

Technology Transfer Assistant

C: [redacted]
AU Office of Sponsored Programs

Doc ID: 6687081

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: RENOIR
Date: Monday, April 13, 2015 9:11:56 AM

Hi,

My name is [redacted] and I am a Research Associate at the Naval Postgraduate School (NPS) in Monterey, CA. I work at the Remote Sensing Center here at NPS, and we are interested in obtaining a version of and/or getting a license to use RENOIR. How would we go about doing that?

Thank you for your time!

[redacted]
(b) (6)
[redacted]
Faculty Associate - Research
Remote Sensing Center / Department of Physics
Naval Postgraduate School | 833 Dyer Road, Building 232 | Monterey, CA 93943
[redacted]

[redacted]

Doc ID: 6687082

(b) (6)

From: [redacted] Civ NWDC, NCTE NOD, R23
To: IAD CCC
Cc: Tech Transfer
Subject: Request for Blue Scope Tool for Navy Enterprise Network Use
Date: Thursday, November 19, 2015 5:34:49 PM

Sirs,
I'm looking for the correct contact at NSA to start communications on obtaining the Blue Scope Tool set for use on the Navy Continuous Training Environment (NCTE) network. I'm the Network Operations Director and our Flag, RADM [redacted] requested that we obtain the Blue Scope tool set to ensure that our network stays CCRI ready year round. I have qualified system administrators and IA specialist that can take any required training for the tool. I would work the government transfer agreement that may be required. Please forward this email to the government representative that handles software use agreements for NSA's Blue Scope tool.

Thanks.

(b) (6)

[redacted] (GS-15)
NCTE Network Operations Director (NOD)
Navy Warfare Development Command (NWDC)
[redacted]

[redacted] for [redacted]

Doc ID: 6687083

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: speaking at science fair
Date: Wednesday, February 11, 2015 7:03:28 PM

Dear NSA,

I'm writing with regards to the Tech Transfer program I heard about when I visited your headquarters as part of the Defense Science Study Group, of which I'm a member. I'm a professor at Stanford and my lab uses nanotechnological tools to investigate the immune system.

When I was there, I asked about the possibility of speaking at my kids' elementary school science fair and your folks mentioned that outreach of this kind was definitely possible. I'm writing to see if you might be able to speak on March 11 on the subject of cryptography. The target audience is K-5 grade (ages 5-11). The forum is our 3rd annual Science Night at Escondido Elementary school, which is a festival of hands-on, interactive scientific exhibits & presentations. Last year we had a cardiologist dissecting a heart, geophysicists showing off earthquakes, astronomers showing off stars and the moon, a robotics team showing off their basketball-shooting robot, etc. It's a lot of fun for the kids to be exposed to so much science and technology. The elementary school services many of the children of Stanford faculty (like me) and my access to Stanford makes it possible to get such awesome speakers & exhibits. Right now, however, math is quite under-represented in our Science Night. We'd love to have a speaker talk about, say, simple substitution ciphers or other topics related to code making or code breaking that young kids would appreciate.

Thanks for your consideration. Please let me know if it can be done.

Sincerely,

(b) (6)

[redacted]

+----------

[redacted] MD PhD
Assistant Professor of Pediatrics - Immunology & Allergy
Stanford University
[redacted]
http://tcell.stanford.edu

[redacted]

Doc ID: 6687084

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: source code access / [redacted]
Date: Monday, April 13, 2015 7:44:36 PM

(b) (3)-P.L. 86-36

I'm working with former NSA employee [redacted] on a project, and he is working with [redacted] to get some source code transferred. Is this a good email address to get in contact with [redacted]?

[redacted]

(b) (6)

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: TTP & websites
Date: Monday, April 20, 2015 1:42:29 PM

Hello,

I recently attended a GovCon event at the Center Club and heard about your TTP. Given the goals of the TTP as stated on the website: https://www.usa.p... /rese ...ch_transfer/partner_benefits/index.shtml I wanted to know what marketing support you provide for the program partners? As the saying goes, building a better mouse trap doesn't necessarily lead to a successful business venture without effective sales and marketing.

My primary interest is in the design/development of websites to support commercial products when they're ready to launch. How is this currently handled?
Who would be the POC to contact to discuss working with your partners?

Regards,

(b) (6)

[redacted]
Graphic Beans
[redacted]
www.graphicbeans.com
Facebook
MD Green Registry Member

[redacted]

Doc ID: 6687086

(b) (6)

From: [redacted]
To: Tech Transfe
Subject: Detecting SIM Card Removal and Reinsertion
Date: Wednesday, May 18, 2016 3:24:37 PM

Hello To all of NSA TEAM!!

We are interested to get more information about Detecting SIM Card Removal technology.

Best Regards

(b) (6)

[redacted] PhD

President

YashaSolar IncNew York City

[redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: TTP information inquiry
Date: Thursday, December 17, 2015 1:07:39 PM

Hello,

I'm an engineer and journalist at The Times interested in information regarding the NSA TPP program. Specifically, I'm interested in looking at existing patent license agreements for NSA technologies. Is there a process through which I can request license agreements as well as the corresponding letters of application and business plans?

Thank you for your time.

(b) (6)

Best,
[redacted]

--
[redacted]
New York Times
[redacted]

[redacted]

Doc ID: 6687088

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Dual Use Tech Transfer
Date: Friday, November 18, 2016 11:07:08 AM

I am [redacted] I work at BMPC. We are trying to develop a plan to secure our instrumentation and control equipment and am interested in seeing what technology is available and can be transferred to our application.

(b) (6)

My number is [redacted]

[redacted]

Doc ID: 6687089

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Upcoming Symposium on Federal Labs/Cooperative R&D - Panelists Needed
Date: Thursday, August 20, 2015 2:49:49 PM

Hi.

We are in the process of putting together a symposium in partnership with NIST that highlights how companies can successfully work with federal labs through cooperative research. The theme of the event is to highlight the importance of innovation to the economy and the role of federal labs as partners/innovators through funding and supporting basic research.

The event will have panel discussions featuring companies that have successfully developed technologies in partnership federal labs through Cooperative Research and Development Agreements (CRADA), Technology Investment Agreements (TIA), Grants, or other transactions. We are interested in areas of big data/analytics, cybersecurity and energy. We are also interested in learning about innovative work of companies in other technology areas as well.

Has the National Security Agency worked with any Fairfax County companies to develop new technologies that might be good panelists? If you have not worked with any Fairfax County companies, do you have any from northern Virginia area who might be good panelists/speakers for our event?

Please feel free to call me if you have any questions.

[redacted]
(b) (6)
Manager, Business Research
Fairfax County Economic Development Authority
8300 Boone Boulevard, Suite 450
Tysons Corner, VA 22182
[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: Your Tech Transfer program
Date: Sunday, November 22, 2015 11:50:53 AM

Dear Sir/Madam,

I'd be interested in knowing more about your Technology Transfer program, and how/if my group could participate.

Below you find all my references and contacts.

(b) (6)

Best regards, [redacted]

[redacted]
Professor of Algorithms
Department of Computer [illegible]
University of Pisa, Italy
www, skype, hangout, link[illegible] twitter

[illegible]ed f[illegible]

Doc ID: 6687091

(b) (6)

From: [redacted]
To: Tech Transfe:
Subject: Accelerated Batch Digital Signature Verification
Date: Monday, November 21, 2016 4:35:01 PM

Hello,

My name is [redacted] with Academic Technology Ventures and I am contacting you on behalf of one of our technology specialist [redacted] with Academic Technology Ventures Inc. (www.academictechventures.com). [redacted] is interested in speaking to you about a technology you currently manage, specifically: ***Accelerated Batch Digital Signature Verification***

(b) (6)

[redacted] is available most days 9 am-5pm EST. Please let me a know day and time that works well for you to discuss this further.

I look forward to hearing from you.

(b) (6)

Thank you,

[redacted]

[redacted]
University Coordinator
Academic Technology Ventures Inc.
[redacted]

The Founders of Plasma Stream Technologies, Inc. - plasmastreamtech.com
As Featured in Popular Mechanics Magazine and NewScientist Magazine

[redacted]

Doc ID: 6687092

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Acquiring Toolsets
Date: Tuesday, May 17, 2016 10:15:12 AM

Good morning,

I am a DoD contractor supporting the Defense Contract Management Agency's (DCMA) Information Assurance Directorate. Given that I have prior Blue Team experience within the DoD, I have been tasked to establish a Blue Team program for DCMA to conduct internal assessments of our network.

I would like to get some information on the possibility and the process of our agency acquiring tools to support this objective. Any information or guidance on this matter would be much appreciated. Thank you.

(b) (6)

Very respectfully,

[redacted]
IA Program Support ICF International
Cyber Security Assessment Team
On Site Supporting:
DCMA Fort Lee, VA
[redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: AUTM Industry Partnering Forum
Date: Tuesday, July 19, 2016 3:05:57 PM
Attachments: AUTM Partner[illegible] Forum proposal.docx

Dear NSA Tech Transfer Colleagues,

Our office at the University of Maryland will be working with the Association of University Technology Managers (AUTM) http://www.autm.net/ to organize Cybersecurity Industry Partnering Forum, similar to these partnering forums: http://www.autm.net/events-courses/autm-partnering-forums/

At this event technology transfer professionals from different universities and research institutions will be able to network with representatives from companies, learn about their cybersecurity needs and present technologies available for licensing. I am attaching an internal proposal giving you more details about the event.

Would you be interested to participate in the event? Would you like to serve on the organizational committee? The committee will be meeting about once a month.

Please let me know if you have any questions or concerns and if you'd like to have a phone call to discuss this further.

Thank you,

(b) (6)

[redacted], MBA'13
Technology Licensing Associate, Information Science
Office of Technology Commercialization
University of Maryland
2130 Mitchell Building
College Park, MD 20742
[redacted]

AUTM Partnering Forum: Cybersecurity

Proposed time: Early June 2017
Location: The Hotel

Reasoning: The University of Maryland, College Park is located in one of the leading areas in the country for cybersecurity innovation and within driving distance of many companies big and small that deal with cybersecurity: Lockheed Martin, Northrop Grumman, Leidos, the federal government and many others. The University is home to the Maryland Cybersecurity Center (MC2) where faculty are performing extensive cybersecurity research, including wireless and network security, cryptography, secure programming, mechanisms for ensuring citizens' privacy in social networks, cyber supply chain research, attacker behavioral analysis, cybersecurity policy, multimedia forensics, and the economics of cybersecurity, among other areas. UMD is uniquely positioned to bring universities and industry together to explore licensing and research opportunities in the area of cybersecurity.

Goals:
7-10 companies
10-12 universities
Sponsorship goal is $4,500 (3 @ $1,500 each).
Registration Revenue is $14,750 (50 @ $295)

AUTM will provide: AUTM will provide help with logistics. AUTM will secure the hotel contract and will plan the logistics of the event with caterers, AV, etc. Where AUTM cannot help is in securing the industry participation. AUTM will market the event to their large database, but UMD and our committee need to do the leg work of personally inviting universities that we know are interested in this sector and contacting industry partners in this space.

UMD responsibilities:

UMD is required to provide the following support and logistics:

- Meeting space (AUTM will negotiate and execute contract)
    - Conference rooms for plenary discussions
    - Exhibit space – tables for each organization represented
    - Space for meals
    - Space for private partnering meetings
- Audio Visual equipment (complimentary or low cost)
- Recommendations for catering services for meals (AUTM will negotiate and execute contract)

- Recommendations for hotel accommodations (AUTM will negotiate hotel reservation contract)
- Ensure availability for the point of contact person responsible (and person implementing if delegated) to work with AUTM staff on coordination of:
    - Meeting
    - Reception
    - Registration
    - All other logistics
- Convene a working committee of 3-8 members
    - Ideally, the committee members would be active in that technology sector and have
    - numerous contacts with companies and universities in that sector.

- Ideally, committee members will be half from industry and half from academia
- Attend regularly scheduled conference calls

• Work with the AUTM staff to secure sponsorship for the meeting

- Current goals are $1,500 in sponsorship per sponsor with a total of $4,500 per event.

Sponsorship goal may need to be higher if the proposal includes extra expenses, such as paying for meeting space or a special event.

OTC Resources required:

- Staff time: approximately 30 hours a month for 10 months
- Marketing budget: $2,500

Doc ID: 6687094

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Contact IETTN - NSA Technologies
Date: Tuesday, June 14, 2016 10:00:56 AM

(b) (3)-P.L. 86-36

Hi [redacted]

(b) (6)

My name is [redacted] editor-in-chief of a brand new IEEE publication meant to promote technology transfer in the field on industrial electronics (IETTN):

http://iettn.ieee-ies.org/

I recently saw this article :

http://www.bizmonthly.com/technology-transfer-at-nsa-innovation-from-lab-to-market/

Do you know if that would be possible to respin this article on IETTN so that we can share it to our audience (there are 450,000 IEEE members) ? This audience is composed on one side of technical people developping technologies and on the other side industrial people developping & financing product development.

Also, I notice that NSA has a lot of industrial electronics technologies:

https://www.nsa.gov/what-we-do/research/technology-transfer/

That would be great to have you as a listed TTO on IETTN:

http://iettn.ieee-ies.org/subscribed-ttos/register-your-tto/

It's free !

Let me know of any interest.

Best Regards, [redacted]

(b) (6)

--
[redacted] ing., Ph.D.
IETTN Editor-in-Chief
IEEE Industrial Electronics Society
[redacted]
Signup here --> iettn.ieee-ies.org

[redacted].pdf

(b) (6)

From: [redacted]
To: Tech Transfe
Subject: CRADA Information
Date: Monday, November 28, 2016 7:37:51 AM

We are looking for more information about joining with NSA for a CRADA on signal processing and analysis to perform a joint effort to further some of NSAs existing tools and apply them to a secondary use case with in commercial cyber security world. Who would be the POC for more information on process to move forward on an effort like this?

Thanks,

[redacted]

(b) (6)

[redacted]

Doc ID: 6687096

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: Data Transfer Agent Training
Date: Thursday, December 08, 2016 8:05:48 AM
Importance: High

(b) (6)

Good morning,

My supervisor [redacted] Director of US Army Aberdeen Test Center's Cyber Security Directorate asked me if I could find out if you offer Data Transfer Agent training. If so, please asvise.

Thank You.

(b) (6)

[redacted]
US Army Aberdeen Test Center
Test Technology Dir. CyberSecurity Div.
Bldg 5014, Room C-4
[redacted]

[redacted]

Doc ID: 6687097

(b) (3)-P.L. 86-36

From: IAD_CCC
To: Tech_Transfe
Cc: [redacted]
Subject: FW: Vulnerability Tool Suite (VTS)
Date: Tuesday, May 17, 2016 2:06:28 PM

Greetings Tech Transfer team,

I've got a request from the International Broadcasting Bureau for a Tool Sharing Agreement of the Vulnerability Tool Suite. I've been provided the following contacts for the agreement.

(b) (6)

Technical POC:
[redacted] Agency Chief Information Officer (CIO);Phone: [redacted] (UNCLASS) [redacted]

Admin POC:
[redacted] - Manager, Insider Threat Program Office): Phone: [redacted] (Office); [redacted] (Mobile); (UNCLASS) [redacted]
If you need anything further please do not hesitate to reach out.

(b) (6)

[redacted]
II:513 - IAD Client Contact Center

(b) (3)-P.L. 86-36

[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, May 09, 2016 7:59 PM
To: IAD_CCC
Cc: [redacted]
Subject: Vulnerability Tool Suite (VTS)

(b) (6)

Dear NSA Information Assurance Directorate (IAD),

On April 1st, 2016, the NSA IAD Client Contact Center (CCC) met with [redacted] and [redacted] of the Broadcasting Board of Governors' (BBG) Information Technology Directorate. They made a presentation about information assurance products and services that could be made available to civilian agencies.

I believe BBG's mission to broadcast to areas of the world in turmoil or under repressive regimes makes BBG a good candidate for some of these products and services. BBG's mission places its information technology and broadcasters in the crosshairs of malicious nation-state sponsored cyber threats. Consequently we believe CCC's Vulnerability Tool Suite (VTS) product would be a good complement to our current cybersecurity tools and defenses. Please advise how we can establish the necessary agreements between BBG and NSA to acquire and operate the VTS product.

Sincerely,

[redacted]

(b) (6)

[redacted]

CIO/CTO

BBG

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: NSA's Detecting SIM Card Removal and Reinsertion
Date: Monday, March 06, 2017 11:48:59 AM

Hello!

My name is [redacted] with Academic Technology Ventures (www.academictechventures.com) and I am contacting you on behalf of one of our technology specialists, [redacted] He is interested in speaking to you about a technology you may currently manage - NSA's Detecting SIM Card Removal and Reinsertion (https://www.federallabs.org/index.php?tray=content&tid=1FLtop199&cid=166DW88)

[redacted] is available most days 8 am-5pm CST. Please let me know day and time that works well for you to discuss this further.

I look forward to hearing from you

(b) (6)

--
Thank you,

[redacted]

[redacted]
University Coordinator
Academic Technology Ventures Inc.
[redacted]

The Founders of Plasma Stream Technologies, Inc. - plasmastreamtech.com
As Featured in Popular Mechanics Magazine and NewScientist Magazine

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: IC Transfer Question
Date: Thursday, March 03, 2016 11:08:15 AM

Good Morning,

I am trying to identify a signer for a TTSA between NSA and the FBI, and am getting hung up on our side with concerns about finding a signer on our side equivalent to the Director, Office of Research and Technology Applications. Can you tell me if that position is a GS level, or SES level position.

Thanks,

(b) (6)

[redacted]
Operational Technology Division
Federal Bureau of Investigation

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: Patent #7,607,958
Date: Tuesday, April 18, 2017 3:08:53 PM

We are interested to get more information on this technology for us to develop/market for commercial use. Please send us the details to start this process thanks.

[redacted]
Vice President
AiNET Corporation
www.ai.net

(b) (6)

[redacted]

Doc ID: 6687101

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Portfolios at FOUO and Higher?
Date: Tuesday, July 11, 2017 6:38:12 PM

Sir/Madam,

I attended the 2017 Baltimore IAS conference, and at the tech transfer booth I spoke with someone who was an NSA employee at the tech transfer book. Unfortunately, she did not have a business card and I lost her contact information.

If it is available, I would like to obtain FOUO and higher tech transfer portfolios.

I am the Cybersecurity Technical Advisor at the undersea resource sponsor (OPNAV N97), and would like to promulgate material to our science advisors, leadership, and other strategic organizations.

The catalyst was a particular set of the public patents caught my attention.

V/r,

[redacted]
OPNAV N972B
Cybersecurity Technical Advisor
[redacted]
Office Location: Pentagon [redacted]
[redacted]

(b) (6)

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Interest in NSA's Data Port Protection and Tamper Detection program
Date: Thursday, November 24, 2016 12:27:49 AM

Hi,

I'm working in the network security field in San Francisco, and am writing to learn more about your Data Port Protection and Tamper Detection program. Can you please point me to some useful resources where I might learn more?

Thank you.

(b) (6)

[redacted]

Varpath
One Market Street
Spear Tower 36th floor
San Francisco, CA 94105

Approved for [illegible]

Doc ID: 6687103

(b)(3)-P.L. 86-36

From:
To: Tech Transfer
Cc: IAD CCC
Subject: Tool Sharing Agreement ICO EPA
Date: Friday, May 06, 2016 10:54:40 AM

Greetings Tech Transfer team,

I've got a request from the EPA for a Tool Sharing Agreement of the Vulnerability Tool Suite. I've been provided the following contacts for the agreement. (b)(6)

Admin POC:
- Senior Agency Information Security Officer (SAISO);Phone: (UNCLASS)

(b)(6)

Technical POC:
- Office of Environmental Information (OEI) Cyber Security Staff (CSS); Phone: (Office);
(Mobile); (UNCLASS) (HSDN) (JWICS)

If you need anything further please do not hesitate to reach out. (b)(3)-P.L. 86-36

Cheers,
Client Advocate
Client Contact Center
Information Assurance Directorate
COMM: NSTS:

for

Doc ID: 6687104

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Presentation Invitation -Block Chain and Distributed Ledgers - Ana Keener, US Army (UNCLASSIFIED)
Date: Friday, November 03, 2017 4:05:29 PM

CLASSIFICATION: UNCLASSIFIED

(b) (6)

To whom it may concern:

On behalf of Major General [redacted] U.S. Army, I would like to invite a representative from NSA's Office of Research and Technology to deliver a presentation to our Command Strategy Group session. This group meets with our commanding general to focus on current and future technology trends. This forum is currently scheduled to meet on Wednesday, 24 January 2018, in Sierra Vista, Arizona.

The topic for this full-day, strategic-level seminar discussion is "Block chain and Distributed Ledgers." The intent of the Command Strategy Group (CSG) would be to identify how Block chain and Distributed Ledgers could be leveraged to further our Cyber capabilities in the defense of our nation's future networks.

(b) (6)

MG [redacted] commands the U.S. Army's Network Enterprise Technology Command, which is headquartered at Fort Huachuca, Arizona and controls all the Army's networks globally. Our mission encompasses the design, engineering, implementation, operation and maintenance required to defend the Army portion of the Department of Defense Information Network (DODIN).

We are seeking executive-level briefers who can engage in discussions on how this Army organization can move forward in the future with technology, processes, procedures, manpower, education and training, along with cooperative engagement with industry, academia and other military service and interagency partners. We can discuss specifics of your presentation at a later day. Preferably in early December.

The CSG is a monthly forum that focuses academic discussion of emerging trends in Information Technology at an executable level. While we see engagements as a relationship-building opportunity with our partners in the science, IT industry and academia, this particular forum is not for acquisition of specific goods or services. On January 24th, our schedule allows 90 minutes (1 hour for presentation, one half hour for questions/comments) for each of our three invited guests to present on the topic. We also invite you to participate in the other two presentations/discussions during the day. We will start at 0800 and conclude before 1530. We will provide means to project slides for discussion, and can bring other supplies upon requests.

I am the appointed "session lead" for this occurrence and you will be able to coordinate directly with me. My contact information is below.

Thank you for your consideration. If your company is not able to participate, any recommendations for organizations that may be interested would be greatly appreciated.

Respectfully,

[redacted] for [redacted]

Doc ID: 6687104

(b) (6)

[redacted] SFPC
ACofS, G2, NETCOM
[redacted]

SMO Collateral: W4NHAA4
SMO SCI: W4NHAA3

CLASSIFICATION: UNCLASSIFIED

Doc ID: 6687105

From: [redacted]
To: Tech Transfe
Subject: TPP
Date: Wednesday, June 15, 2016 1:24:09 PM

(b)(3)-P.L. 86-36

Is there a book version of the PDI ?

(U//FOUO) [redacted] T99
C|CISO, C|EH, E|CSA, Security
Information Security Engineering Senior Professional, ISSG
EISSC Monitoring Desk
Contractor (Eagle Alliance)
[redacted]

[redacted]

Doc ID: 6687106

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Presentation on open-source tools to ISSA Chapter
Date: Thursday, June 22, 2017 1:33:17 PM

Hello,
I was excited to read that NSA has open sourced a number of projects on GitHub. Do you have someone that would come to DC and discuss this portfolio at one of our monthly ISSA Chapter meetings? I think it would be very helpful to our members to find out about all the tools that are available from NSA.

By way of introduction, I am the VP for Programs for the Washington DC Chapter of ISSA (www.issa-dc.org). The Information Systems Security Association is a non-profit association of IT Security practitioners. We invite SMEs to present on topics of interest at our monthly meetings. We meet the third Tuesday of each month at the Center for American Progress (1333 H St. NW) in downtown Washington, DC. 8/15, 9/19, and 10/17 are all currently available.

(b) (6)

Regards,

[redacted]

[redacted]
Vice President, Programs
National Capital Chapter
Information Systems Security Association (ISSA)
www.issa-dc.org
[redacted]

Approved for [redacted]

Doc ID: 6687107

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: TTSA Agreement Information
Date: Thursday, November 17, 2016 1:39:02 PM

Good morning,

I am inquiring for contact information in relation to Technology Transfer Sharing Agreements (TTSA), Cooperative Research and Development Agreements (CRADA), or Open Source Software Releases (OSS) agreements that our organizations/tenants may have established in the past and are valid, before we pursue our own effort.

Could you please tell me if there are existing agreements s in place for the following organizations and provide POCs?

24 Air Force
688 IOW, Information Operations Wing or 688 CW, Cyber Wing
318 IOG, Information Operations Group or 318 COG, Cyber Operations Group
90 IOS, Information Operations Squadron or 90 COS, Cyber Operations Squadron
92 IOS, Information Operations Squadron or 92 COS, Cyber Operations Squadron
346 TS, Test Squadron
23 IOS, Information Operations Squadron
318 OSS, Operations Support Squadron

(b) (6)

V/r,

[redacted] CIV, USAF
AFSPC 318 OSS/OSK, Weapons and Tactics
[redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Question about new GitHub page
Date: Thursday, June 22, 2017 10:06:41 AM

Hi there,

My name is [redacted] and I'm a reporter at FedScoop. I noticed that the NSA recently launched a GitHub page and would love to hear more about it — when did the agency launch the GitHub page? And why did the NSA decide to join GitHub in an official capacity at this time?

Thanks,

(b) (6)

[redacted]

--

[redacted]
Technology Reporter, FedScoop
Scoop News Group
FedScoop//StateScoop//EdScoop//CyberScoop

[redacted]

[redacted]

Doc ID: 6687109

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: USB and Data Port Protection
Date: Tuesday, September 20, 2016 10:31:42 AM

NSA Team.
1. Strategic Systems Program (SSP) - SP24 Navigation Branch request information regarding the use of USB and Data Port Protection technology for use on SP24 Navigation laptops
2. Please advise as to availability, cost and procurement process for port protection devices. Are samples available for assessment prior to purchase.

(b) (6)

V/R,
[redacted] SP2432
SP24 Navigation - Cybersecurity ISSM
[redacted]

[redacted]

Doc ID: 6687110

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: RE: Malaysia Tender - Proposed Product & Quantity
Date: Tuesday, April 18, 2017 12:39:44 AM

Sir/Madam,

I am pleased to bring to the notice of your company, an available tender for the supply of your products line to the government of Malaysia through a tender.

I would like to know if your company will be interested to submit offer for this supply.

Please confirm your interest and I will give you more information about the tender as soon as I read positively from you

N/B PLS KINDLY RESPOND ONLY ON THIS EMAIL ADDRESS BELOW:

Email; [redacted]

(b) (6)

Thank you,

[redacted]

[redacted]

Doc ID: 6687111

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: MULTIMEDIA INSTRUCTIONAL DESIGN SYSTEM / DIGITAL TRANSCRIPTION SYSTEM (SCRIBEZONE™)
Date: Wednesday, March 01, 2017 5:46:45 PM

Hello!

(b) (6)

My name is [redacted] with Academic Technology Ventures and I am contacting you on behalf of one of our technology specialists, [redacted]. (www.academictechventures.com) [redacted] is interested in speaking to you about a technology you may currently manage - MULTIMEDIA INSTRUCTIONAL DESIGN SYSTEM / DIGITAL TRANSCRIPTION SYSTEM (SCRIBEZONE™) (https://www.nsa.gov/what-we-do/research/technology-transfer/assets/files/nsa-technology-transfer-program.pdf). Please locate PAGE 30 in the catalog.

Will is available most days 9 am-6 pm EST. Please let me know day and time that works well for you to discuss this further.

I look forward to hearing from you.

(b) (6)

--
Thank you,

[redacted]

[redacted]
University Coordinator
Academic Technology Ventures Inc.
[redacted]

The Founders of Plasma Stream Technologies, Inc. - plasmastreamtech.com
As Featured in Popular Mechanics Magazine and NewScientist Magazine

[redacted]

Doc ID: 6687112

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: RENOIR Info Request
Date: Thursday, April 20, 2017 10:41:54 AM

Classification: UNCLASSIFIED

To Whom It May Concern:

As Senior Data Scientist under contract to NGA's Office of Science & Methodologies. I am requesting the latest version of the RENOIR software tool along with a user manual, and a technical reference description of the tool's use and capabilities with examples for Network and Cluster Analysis.

Thanks much I appreciate your help.

(b) (6)

[redacted] Ph.D.
Data Scientist
ATSGB/NCE
[redacted]
S61339

Classification: UNCLASSIFIED

Approved for [redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: NSA + Wellspring - FLC 2017
Date: Wednesday, April 19, 2017 3:16:24 PM

Hello,

Great to see that the NSA is attending the FLC Annual meeting this year! As an organization with a robust tech transfer office, I know how important things such as automation, visibility, and sophisticated reporting are to the agency.

I'm not sure how familiar you may be with Wellspring, but we've successfully helped over 200 universities and research institutions enhance their tech transfer activities. As a result, a recent Association of University Technology Managers (AUTM) survey has shown that Wellspring Sophia clients report 46% more licensing revenue and filed 34% more patents.

I wanted to see if you would be available for a 15-minute meeting during FLC 2017. We'd love to learn more about your Technology Transfer activities as well as to share some exciting new enhancements to Wellspring's Sophia and our recent migration of Flintbox, a Wellspring solution, with the AUTM Global Technology Portal.

Would you be interested in connecting for 15 minutes?

Best,

[redacted]

(b) (6)

--

[redacted]
Director of Business Development Wellspring
350 N. LaSalle, Ste. 1200, Chicago, IL 60654

[redacted]

Schedule a Call with [redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfe
Subject: Seeking info
Date: Wednesday, June 21, 2017 6:55:38 AM

Sir,

How could I work for some NSA project and contribute to some project launched by NSA .

Appr[illegible] for [illegible] by NSA [illegible]

Doc ID: 6687115

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: NSA Technology Transfer Program (TTP)
Date: Tuesday, June 27, 2017 8:29:31 AM

Good morning,

I have worked closely with Fort Meade for the last 10 years. I would like to talk to someone about the TTP program and how I can help you sell more of your patents

Please let me know who I should talk to,

Thanks,

(b) (6)

[redacted]
Meadowgate Technologies, LLC
[redacted]

[redacted]

Doc ID: 6687116

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: small question on your git projects
Date: Wednesday, June 21, 2017 9:31:30 PM

To Whom It May Concern,

I noticed that of all the projects you folks placed on GitHub, nothing in the area of A.I.? Do you folks have any public domain stuff in the area of A.I. Question Generation? It would be cool to see something like that on your GitHub page.

(b) (6)

Cheers,

[redacted]

[redacted] for [redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [EEMSG: Marketing][Non-DoD Source] 2017 Gartner Magic Quadrant for IT Vendor Risk Management
Date: Thursday, July 13, 2017 8:03:27 PM

(b) (3)-P.L. 86-36

Dear [redacted]

Download the 2017 Gartner Magic Quadrant for IT Vendor Risk Management report now

In recent times, unmanaged risks from IT vendors have exposed organizations to data breaches, operational failures, and business disruptions resulting in huge financial losses and reputational damages. Moreover, regulations like OCC, PCI-DSS, GLBA, HIPAA Rule, and HITECH Act are focusing on greater accountability and better oversight on the governance of vendor relationships. This has made it imperative for organizations to proactively consider IT VRM solutions that effectively help mitigate the risks caused by IT vendors.

Here is a complimentary copy of the latest Gartner Magic Quadrant for IT Vendor Risk Management Report that will give you a comprehensive overview of the IT Vendor Risk Management (VRM) solution landscape.

Access the complimentary copy of the Gartner report today.

(b) (6)

Best Regards,
[redacted]
Marketing Team

Governance, Risk, Compliance and Quality Management Solutions

MetricStream sends email to those individuals who have provided permission to send ongoing communication via email.
If you do not wish to receive ongoing communication via email from MetricStream: Unsubscribe

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] Need Patent License Info about Elliptic Curve Cryptography
Date: Wednesday, July 12, 2017 5:44:35 PM

Hi,

I am learning about ECC and have come across many web links to an NSA page that is supposed to be about licensing the ECC patents license from Certicom (Blackberry).

The page does not seem to exist and all I can find is the Transfer Technology PDF which only seems to cover NSA patents.

Can you point me to a list of the ECC patents that are licensed for use?

I found open source software I want to test but I want to make sure it doesn't seem to infringe on any of the patents. If so, I'll have to get our legal and purchasing people involved, but I only have authority to inquire about the types of patent licenses available.

Thanks,

(b) (6)

[redacted]
NNL
[redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] Data Port Protection and Tamper Detection
Date: Wednesday, September 20, 2017 5:41:30 PM

Hello,
My name if [redacted]. I work for Tru Simulation + Training as an Air Force Contractor. I was wondering if I could get a little more info regarding the Data Port Protection and Tamper Detection application, specifically how much it costs, how it's deployed, and if it would work on RJ45 ports.

Thank you.

[redacted]
Cyber Security Specialist
Tru Simulation + Training
[redacted]

(b) (6)

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] Requesting access to Data Tool for..
Date: Friday, August 18, 2017 12:16:03 PM

Dear Tech Transfer @ NSA.

https://www.nsa.gov/what-we-do/research/technology-transfer/assets/files/identifying-connected-data.pdf

Here are my questions:
I really need tool that does what it states in that description.

Is there a development version for demoing and testing?
What's the licensing cost?
Training?
Does it work with Oracle PL/SQL, Microsoft SQL Server, MongoDB, or PostGreSQL?

(b) (6)

[redacted]
Homeland Security Division
National & Homeland Security
Idaho National Laboratory | 5 North Fremont Ave. | Idaho Falls, ID 83415-3790
[redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] DHS Patent Pool Inquiry
Date: Wednesday, July 19, 2017 11:16:34 AM
Attachments: image001.png

Good Afternoon,

I am working in a supporting role for DHS in their Office of University Programs. Much like The NSA, we partner with Universities across the country to help expand knowledge and capabilities. We are interested in developing a patent pool (licensing program) to help commercialize our Universities efforts. Would it be possible to speak with someone regarding The NSA's licensing program, and maybe more specifically, how The NSA's COEs are integrated into the program? Thank you in advance.

(b) (6)

Best Regards,

[redacted]

[redacted]
Support Contractor
Department of Homeland Security
Science & Technology Directorate
Office of University Programs
[redacted]

Homeland Security

Approved for [redacted]

Doc ID: 6687122

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: [Non-DoD Source] Request License US Patent 09812836
Date: Tuesday, December 19, 2017 1:12:55 PM

National Security Agency
ATTN: Technology Transfer Program
9800 Savage Rd., Suite 6843
Ft. George G. Meade, MD 20755-6843
Telephone: (866) 680-4539
tech_transfer@nsa.gov

Hi.

Request License for US Patent 09812836
https://www.google.com/patents/US9812836

Please inform procedure.

US Patent 09812836
Reversible computation with flux solitons
Abstract: A reversible superconducting circuit includes a plurality of Josephson transmission lines. A first line is configured to transmit a control fluxon when a first input is active. A second line is configured to transmit a target fluxon to one of a third â€¦ [more]
Inventors: Kevin D. Osborn
Assignees: The United States of America as represented by the Director, National Security Agency
Publication number: 09812836
Publication date: Nov 07, 2017
Application number: 14121007
https://patents.justia.com/patent/09812836

(b) (6)

Thanks
[redacted] Founder start-up EETAI
Menlo Park, California

[redacted]

Doc ID: 6687123

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] Getting started with the TTP
Date: Friday, November 17, 2017 1:00:11 AM

To Whom It May Concern:

I enjoyed pursuing through your website. I am ready to speak with a representative regarding the proper steps to begin partnership with the CRADA (Cooperative Research and Development Agreement). Please correspond via email, [redacted]

(b) (6)

Regards,

[redacted] CEO
International PROOF Systems, LLC
PROOF Smart Tags
www.InternationalPROOFSystems.com
[redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfe
Subject: [Non-DoD Source] ScribeZone(R): A Multimedia Instructional Design System
Date: Wednesday, July 19, 2017 1:17:52 PM

Hello!

I sent an email quite awhile ago expressing Academic Technology Ventures' interest in a technology you may currently manage -

ScribeZone®: A Multimedia Instructional Design System

> **ScribeZone®: A Multimedia Instructional Design System Device for and Method of Language Processing US PATENT # 8,380,485 | EXPIRES AUGUST 11, 2031 ScribeZone® is an educational technology that facilitates development and delivery of interactive multimedia courseware for the classroom. ScribeZone® enables instructors to synchronize multimedia files with their corresponding written texts and then divide the media into manageable learning blocks to appropriately focus and challenge their learners. Instructors can customize and frame courseware with hints, glossaries, and links to outside resources. ScribeZone® presents the multimedia courseware and its sophisticated media playback system in one window, making course materials easy to develop, access, navigate, and complete. POTENTIAL APPLICATIONS: • K-12 and higher education • Foreign language and English as a Second Language (ESL) courseware development • Government, military, and law enforcement applications • Medical and legal transcription and translation • Media and broadcasting**

Our Technology Specialist, Mr. [redacted] is still interested in discussing this further and any licensing opportunities that may still be available. Please feel free to send an NDA if needed. He is open to take a call most any day Monday through Friday from 8-5 EDT.

Please let me know a good day and time that works well for you to have a call.

I look forward to hearing from you

(b) (6)

--
--
Thank you,

[redacted]

University Coordinator
Academic Technology Ventures Inc.

[redacted]

The Founders of Plasma Stream Technologies, Inc. - plasmastreamtech.com
As Featured in Popular Mechanics Magazine and NewScientist Magazine

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] Innovation
Date: Monday, November 13, 2017 4:35:19 PM

Hello Tech Transfer,

I'm [redacted], former FAO/R&T analyst for over 10 years stationed at both Hawaii and Texas sites. I am now the security architect for an electrical utility in San Antonio, Texas. I am reaching out to you to inquire how our innovation's team who are already working with local colleges (UTSA) and other entities can collaborate new ideas, research, innovation with **your team**? If I could please be put in contact with someone to start that process and have those preliminary discussions that would be magnificent.

(b) (6)

[redacted]
Security Architect | I
CPS Energy | 145 Na San Antonio, Texas 78205
[redacted]
cpsenergy.com

Approved for [redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] TTSA software
Date: Friday, August 11, 2017 4:12:47 PM

Hello. I am trying to find a contact to learn how I get a copy of some NSA testing tools for use in an unclass environment. I am not sure what the process is or how long it takes to get access. Any detail or POC would be greatly appreciated.

[redacted]

(b) (6)

[redacted]

[redacted]

[redacted]

Doc ID: 6687127

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] licensing position
Date: Friday, September 29, 2017 6:08:21 PM

Hello,

I am looking for the correct place to inquire about employment opportunities with NSA technology transfer.

Is there a place I can go to become aware of current and/or future opportunities?

Thanks,

--

(b) (6)

[redacted]

[redacted]

Doc ID: 6687128

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] US PATENT # 8,177,089 Reusable Tamper-Indicating Tube
Date: Friday, November 10, 2017 10:11:31 PM

Hello NSA,

I am an inventor and small business entity. I would like to opportunity to speak with you in regards to a technology transfer of US PATENT # 8,177,089 Reusable Tamper-Indicating Tube. It's something I can believe in and a product that a small business can handle. Please contact me at your earliest.

(b) (6)

[redacted]
US Patent 9,609,973
PCT Application US17/21183

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] Inquiring about the process regarding partnership with the TTP
Date: Friday, October 06, 2017 3:04:50 PM

To Whom It May Concern:

My name is [redacted] and I would like to receive additional information regarding partnership with the NSA Technology Transfer Program. Please feel free to correspond via email, [redacted]

Regards,

(b) (6)

[redacted] CEO
International PROOF Systems, LLC
PROOF Smart Tags
www.InternationalPROOFSystems.com
[redacted]

[redacted]

Doc ID: 6687130

(b) (6)

From: [redacted]
To: [redacted] (b) (3)-P.L. 86-36
Cc: [redacted] Tech Transfer
Subject: Date Confirmation CSG Session - Block Chain and Distributed Ledgers (UNCLASSIFIED)
Date: Thursday, December 21, 2017 12:33:46 PM

CLASSIFICATION: UNCLASSIFIED

Good Morning [redacted]

I assume you are already out and won't receive this email until your return.
I have cc:'d the team members you requested I include during your absence.

(b) (6)

Major General [redacted] staff secretary has confirmed the January 24, 2018 date for the CSG Session. The exact time will follow.

Any question or concerns please let me know.

Have a wonderful holiday!

Respectfully,

[redacted] SEPC
ACofS, G2, NETCOM
[redacted]

SMO Collateral: W4NHAA4
SMO SCI: W4NHAA3

CLASSIFICATION: UNCLASSIFIED

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: [Non-DoD Source] NC State technology transfer inquiry: Flexible circuit
Date: Sunday, September 10, 2017 8:50:16 PM

Tech transfer team.

I am a graduate student at NC State University in the TEC program on a team interested in commercialization of the Flexible Circuit technology that is listed in the NSA Patent Portfolio (Patents #7,452,746 & #6,017,822). We are hoping to get in touch with the technologists inventors and get some more information on the progress and capabilities of the technology.

I've also copied members of my team to see the conversation. Let us know what we can do to help facilitate this communication process.

(b) (6)

Thanks.

[redacted]

--

[redacted]
Graduate Student

[redacted]

Doc ID: 6687132

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: [Non-DoD Source] Meeting on technology transfer
Date: Tuesday, September 12, 2017 10:44:43 AM

Good Morning,

As an introduction, EmeSec is a small cybersecurity company headquartered in Northern Virginia. We are working with government contractor companies to secure their systems in compliance with the new NIST 800-171 and associated DFARs clauses We reviewed the technology transfer website and think there are several technologies that we could use to assist them to further secure their systems with some additional R&D. How do we go about finding out what is required to license these technologies or create a CRADA to work with you to extend the capabilities of these technologies and commercialize them?

(b) (6)

Thanks,

[redacted]

[redacted]

Doc ID: 6687133

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: [Non-DoD Source] Re: NC State technology transfer inquiry: Flexible circuit
Date: Thursday, September 21, 2017 9:06:44 PM

Hi,

Is there is any update on getting in touch with the technologists/inventors for the "Flexible Circuit" technology listed in the NSA Patent Portfolio? We have a few questions about the technology we are wanting to get answered as soon as possible.

Thanks,

(b) (6)

[redacted]

On Sun, Sep 10, 2017 at 8:50 PM, [redacted] wrote:

Tech transfer team,

I am a graduate student at NC State University in the TEC program on a team interested in commercialization of the Flexible Circuit technology that is listed in the NSA Patent Portfolio (Patents #7,452,746 & #6,017,822). We are hoping to get in touch with the technologists/inventors and get some more information on the progress and capabilities of the technology.

I've also copied members of my team to see the conversation. Let us know what we can do to help facilitate this communication process.

Thanks,

(b) (6)

[redacted]

[redacted]

--

[redacted]

Graduate Student

[redacted]

[redacted]

(b) (6)

From: [redacted]
To: Tech_Transfer
Subject: Fw: CRADA Renewal Request
Date: Monday, June 12, 2017 9:23:38 AM
Attachments: Fully Executed MO CRADA 04-28-12.pdf

From: [redacted] (b) (6)
Sent: Tuesday, June 6, 2017 09:47
To: tech_transfer@nsa.gov
Subject: CRADA Renewal Request

Good morning,

We are requesting to renew a previously executed CRADA agreement (see attached).

Request contact information for the appropriate administrative coordination POC.

Very respectfully,

(b) (6)

[redacted]
DIRECTOR, C4ISR PROGRAMS & TECHNOLOGIES
MODUS OPERANDI, INC.
[redacted]
www.modusoperandi.com

[redacted]

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687134

(b)(3)-P.L. 86-36
(b)(4)
(b)(6)

Page Denied

Doc ID: 6687135

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Documentation / Pamphlets for Exhibitors
Date: Thursday, March 02, 2017 3:13:12 PM

Tech Transfer,

We will be hosting an booth at the National Cyber Summit in Huntsville, AL, 06-08 June 2017. In an effort to present as much information about NSA as possible, we were wondering if you had any flyers/pamphlets/hand-outs we could put on the table? Or do you have someone you normally send to events like this that wouldn't mind going and sharing our booth?

Any information would be greatly appreciated.

V/R,

(b) (6)

[redacted]
National Information Assurance Education and Training Program (NIETP)
Attn: E73, 6704
9800 Savage Road
Fort Meade, Maryland 20755-6074

[redacted]

National Information Assurance Education and Training Program
https://www.iad.gov/NIETP/

CAE Community Website
https://www.caecommunity.org

[redacted]

Doc ID: 6687136

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Github page
Date: Thursday, June 22, 2017 11:45:23 AM

Hey friends,

I'd like to draft a story for our website about your new Github page.

Has the public affairs office cleared any statements from the T2 office that we could use?

Thanks,

(b) (6)

[redacted]
Senior Writer/Editor - TechLink
[redacted]
Techlinkcenter.org

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Cc: [redacted]
Subject: TTSA question
Date: Friday, January 13, 2017 10:20:44 AM

Aloha,

I recently took over SSC PAC's T2 office, so still learning some of the ropes. This week I had an inquiry from an employee that I could not answer, so turning to you all for help.

Basic question is who can sign as a leadership POC for your TTSAs? Ie what level are you looking for, first level, second level management/supervision, SES, Commanding Officer....

Short background: Our researcher is working with Sandia National Laboratory to create a suite of software tools that can be used to conduct cyber-testing of IP-based systems. As part of this project they intend to use software that was originally developed by NSA and is being made available to use through a Technology Transfer Sharing Agreement (TTSA). So in order to get access to the software we need to fill out and submit the TTSA....

For additional learning and a chance to improve our office, can I learn more about your Technology Transfer Sharing Agreements (TTSA)? It might not be an option in the DoD, but never hurts to learn more about what others are doing in the T2 arena.

Thank you for your time

(b) (6)

[redacted]

ORTA/T2 Office

[redacted]

[redacted]

Doc ID: 6687138

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: TWO TECHNOLOGIES TO DISCUSS
Date: Wednesday, March 08, 2017 1:06:22 PM

Hello!

My name is [redacted] with Academic Technology Ventures (www.academictechventures.com) and I am contacting you on behalf of one of our technology specialists, Mr. [redacted] He is interested in speaking to you about two technologies you may currently manage:

1. CRYPTOGRAPHIC KEY EXCHANGE USING EFFICIENT ELLIPTIC CURVE Page 15 of catalog
2. DATA RELATIONSHIP AND VISUALIZATION TOOL (RENOIR) Page 38 of catalog

[redacted] is available most days 8 am-5pm MST. Please let me know day and time that works well for you to discuss this further.

I look forward to hearing from you.

(b) (6)

--
Thank you,
[redacted]
[redacted]
University Coordinator
Academic Technology Ventures Inc.
[redacted]

The Founders of Plasma Stream Technologies, Inc. - plasmastreamtech.com
As Featured in Popular Mechanics Magazine and NewScientist Magazine

[redacted]

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Inquiry about nationalsecurityagency.github.io
Date: Monday, June 19, 2017 9:22:50 AM

Hello,

I'm writing this on behalf of Fossbytes, a growing technology media website that extensively covers the developments from open source and security world. A couple of hours ago I spotted this website (https://nationalsecurityagency.github.io/) on the Hacker News and I wondered if it was a new website from NSA. I also read a report from The Next Web that wrongly mentioned that "now" NSA has a GitHub account. I wished to inquire about the same. It would great if you could tell me more about the https://nationalsecurityagency.github.io/ website, its purpose, age, and NSA's future plans to contribute to open source.

(b) (6)

[redacted]
Co-founder & Editor-in-chief, fossBytes
Email: [redacted]

Approved for [redacted]

Doc ID: 6687142

From: MATIS ??
To: Tech Transfer
Subject: SPECK
Date: Tuesday, July 11, 2017 12:30:57 AM

(b) (6)

Hello

My name is [redacted]

I am engaged in MATIS Inc. and our office is located in Tokyo Japan.
We are developing IoT based products such as power consumption measure and control system , Intrusion Detection system in the railway etc.
We intend to implement authentication and encryption function into our product with lightweight encryption algorithm.
We found the SPECK in the lightweight encryption evaluation report published by NICT Japan. NICT Web site is as follows.

http://cryptrec.go.jp/topics/cryptrec_20170630_c16report.html

In the report various encryption algorithms was listed , we felt that SPECK is the most appropriate encryption algorithm for our products.

We want to know about SPECK and we hope a sample source code of SPECK.
Please let me know if it is acceptable or not.

We are very sorry but MATIS was instituted in December 2016 and does not have
Web site until now.
MATIS is the subsidiary company of MTES and its Web site is as follows.

http://mte-s.co.jp/index_eng.html

(b) (6)

Best Regards,

[redacted]
MATIS Co., LTD
[redacted]
Chuo-ku, Tokyo, Japan
[redacted]

[redacted]

Doc ID: 6687143

(b) (6)

From: [redacted]
To: Tech Transfer
Subject: Tech Transfer Resources
Date: Monday, January 23, 2017 2:57:31 PM

Good afternoon,

I came across your technology transfer program and would like to inquire about a couple of the agreements

The TTSA to be more specific; and the CRADA. Any information about the agreements and the process would be greatly appreciated. Thanks!

V/r,

(b) (6)

[redacted]
IT Specialist/MGF Lab Manager
MGF Infrastructure Team
SPAWAR Systems Center Pacific
[redacted]

[redacted]